Proc. London Math. Soc. (3) 121 (2020) 1531–1578 doi:10.1112/plms.12379

Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication

John Coates and Yongxiong Li

Abstract

The paper uses Iwasawa theory at the prime $p = 2$ to prove non-vanishing theorems for the value at $s = 1$ of the complex L-series of certain quadratic twists of the Gross family of elliptic curves with complex multiplication by the field $K = \mathbb{Q}(\sqrt{-q})$, where q is any prime $\equiv 7 \bmod 8$. Our results establish some broad generalizations of the non-vanishing theorem first proven by Rohrlich using complex analytic methods. Such non-vanishing theorems are important because it is known that they imply the finiteness of the Mordell–Weil group and the Tate–Shafarevich group of the corresponding elliptic curves over the Hilbert class field of K. It is essential for the proofs to study the Iwasawa theory of the higher dimensional abelian variety with complex multiplication which is obtained by taking the restriction of scalars to K of the particular elliptic curve with complex multiplication introduced by Gross.

1. *Introduction*

Let $K = \mathbb{Q}(\sqrt{-q})$ be an imaginary quadratic field, where q is any prime number with $q \equiv 7 \bmod 8$. We fix throughout an embedding of K into $\mathbb{C}$. Let $\mathcal{O}_K$ be the ring of integers of K, and write h for the class number of K. Note that, since $q \equiv 7 \bmod 8$, the prime 2 splits in K, say $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, a fact which will underly all of our subsequent arguments with Iwasawa theory. We fix one of these primes $\mathfrak{p}$, and we assume from now on that we have chosen the sign of $\sqrt{-q}$ so that $\mathrm{ord}_{\mathfrak{p}}((1-\sqrt{-q})/2) > 0$. Let $H = K(j(\mathcal{O}_K))$ denote the Hilbert class field of K, where j denotes the classical modular function. Gross [21, Theorem 12.2.1] has proven that there exists a unique elliptic curve A defined over $\mathbb{Q}(j(\mathcal{O}_K))$, with complex multiplication by $\mathcal{O}_K$, minimal discriminant $(-q^3)$, and which is a $\mathbb{Q}$-curve in the sense that it is isogenous over H to all of its conjugates. An explicit equation for A over H is given by

$$y^2 = x^3 + 2^{-4}3^{-1}mqx - 2^{-5}3^{-3}rq^2, \tag{1.1}$$

where $m^3 = j(\mathcal{O}_K)$, and $r^2 = ((12)^3 - j(\mathcal{O}_K))/q$ with $r > 0$ (see [22]). Let $L(A/H, s)$ be the complex L-series of A/H, and write $L(A/H, \eta, s)$ for the twist of this L-series by any finite-order abelian character η of H. For $1 \leqslant n \leqslant \infty$, let $A_{\mathfrak{p}^n}$ be the Galois module of $\mathfrak{p}^n$-division points on A, and define $\mathfrak{F}_\infty = H(A_{\mathfrak{p}^\infty})$. Let $\mathcal{G}$ denote the Galois group of $\mathfrak{F}_\infty$ over H. The action of $\mathcal{G}$ on $A_{\mathfrak{p}^\infty}$ defines an isomorphism $\rho_{\mathfrak{p}} : \mathcal{G} \simeq \mathcal{O}_{\mathfrak{p}}^\times = \mathbb{Z}_2^\times$, where $\mathcal{O}_{\mathfrak{p}}$ denotes the ring of integers of the completion of $\mathcal{O}_K$ at $\mathfrak{p}$.

Theorem 1.1. *Assume that q is any prime such that $q \equiv 7 \bmod 16$. Then, for all characters ν of finite order of $\mathcal{G} = Gal(\mathfrak{F}_\infty/H)$, we have $L(A/H, \nu, 1) \neq 0$.*

Received 30 January 2019; revised 4 May 2020; published online 18 August 2020.

2010 *Mathematics Subject Classification* 11G23 (primary), 11G05, 11G40 (secondary).

The second author is supported by NSFC-11901332.

We remark that, in the special case when ν is the trivial character, Rohrlich [28] has proven that $L(A/H,1) \neq 0$ for all primes $q \equiv 7 \bmod 8$, by a completely different method using complex analytic arguments. However, it does not seem that his method can easily be extended to proving the non-vanishing of the $L(A/H,\nu,1)$ for all characters ν of finite order of $\mathcal{G}$ when $q \equiv 7 \bmod 16$, and we do not know if this stronger assertion is even true for the primes $q \equiv 15 \bmod 16$ (but see [29], where it is shown, in particular, that $L(A/H,\nu,1) \neq 0$ for all but a finite of characters ν of finite order of $\mathcal{G}$ for all primes $q \equiv 7 \bmod 8$). If J is any extension of H, we write, as usual, $A(J)$ for the group of J-rational points on A, and $Ш(A/J)$ for the Tate–Shafarevich group of A/J. In [21], Gross proved that $A(H)$ is always finite. Parallel to Theorem 1.1, we prove the following result.

THEOREM 1.2. *Assume that q is any prime with $q \equiv 7 \bmod 16$. Then, for all finite extensions J of H contained in $\mathfrak{F}_\infty$, both $A(J)$ and the $\mathfrak{p}$-primary subgroup of $Ш(A/J)$ are finite.*

We remark, however, that, when $q \equiv 7 \bmod 16$, and in addition there is more than one prime of H lying above $\mathfrak{p}$, then we show later (see Theorem 8.1) that we always have $Ш(A/\mathfrak{F}_\infty)(\mathfrak{p}) = (K_\mathfrak{p}/\mathcal{O}_\mathfrak{p})^{m_q}$ for some integer $m_q > 0$. On the other hand, it is already well known by an Euler system argument due to Kolyvagin–Gross–Zagier that $L(A/H,1) \neq 0$ implies that both $A(H)$ and $Ш(A/H)$ are finite.

We further prove a non-vanishing theorem for the values at $s = 1$ of the complex L-series of a large class of quadratic twists of A. Let $\mathscr{R}$ denote the set of all square free positive integers R of the form $R = r_1 \dots r_k$, where $k \geqslant 0$, and $r_1, \dots, r_k$ are distinct primes such that (i) $r_i \equiv 1 \bmod 4$, and (ii) r_i is inert in K, for $i = 1, \dots, k$. For $R \neq 1 \in \mathscr{R}$, let $A^{(R)}$ be the twist of A by the quadratic extension $H(\sqrt{R})/H$. Note that such an extension is non-trivial since K has odd class number. We write $L(A^{(R)}/H, s)$ for the complex L-series of $A^{(R)}/H$. By Deuring's theorem, $L(A^{(R)}/H, s)$ is a product of Hecke L-series with Grossencharacter. We shall prove the following theorem.

THEOREM 1.3. *Assume $q \equiv 7 \bmod 16$. Then, for all $R \in \mathscr{R}$, we have $L(A^{(R)}/H, 1) \neq 0$.*

COROLLARY 1.4. *Assume $q \equiv 7 \bmod 16$. Then, for all $R \in \mathscr{R}$, both $A^{(R)}(H)$ and $Ш(A^{(R)}/H)$ are finite.*

Indeed, it is well known (see [24, § 5]) that if E is any twist of A by a quadratic extension of K, then $L(E/H,1) \neq 0$ implies that both $E(H)$ and $Ш(E/H)$ are finite. However, at a much more elementary level exploiting the fact that the torsion subgroup of $A^{(R)}(H)$ is equal to $\mathcal{O}_K/2\mathcal{O}_K$, it has been shown independently by several authors (Choi [4], and Li and Ren [26]) that a classical 2-descent argument on $A^{(R)}/H$ proves that $A^{(R)}(H)$ is in fact finite for all $R \in \mathscr{R}$. However, such an argument tells us nothing about the finiteness of even the 2-primary subgroup of the Tate–Shafarevich group $Ш(A^{(R)})$ for $R \in \mathscr{R}$. We remark that for the special case $q = 7$, the curve A is the modular elliptic curve $X_0(49)$, and the above theorem is already proved in [11] by two rather different methods. In fact, we use a modification of one of these methods, due originally to Zhao [31, 32], to prove the above theorem. However, the proof is considerably more delicate when $q > 7$, and makes essential use of the restriction of scalars abelian variety and its quadratic twists.

Let $\beta = \sqrt{-q}$, and let $A^{(-\beta)}$ be the twist of A by the quadratic extension $H(\sqrt{-\beta})/H$. Thus $A^{(-\beta)}$ is also an elliptic curve defined over H with complex multiplication by $\mathcal{O}_K$. These elliptic curves $A^{(-\beta)}$ seem, in some sense, to be even simpler than the Gross curves A, and they appear not to have been discussed in earlier literature. From equation (1.1) for A, one easily shows that $A^{(-\beta)}$ has the nice explicit equation

$$y^2 = x^3 - 2^{-4}3^{-1}(j(\mathcal{O}_K))^{1/3}x + 2^{-5}3^{-3}(j(\mathcal{O}_K) - (12)^3)^{1/2}, \tag{1.2}$$

where it is understood that, in this equation, we take the real cube root of $j(\mathcal{O}_K)$, and the square root of $j(\mathcal{O}_K) - (12)^3$ lying in the upper half complex plane. Note that this curve is defined over H, but it is not a $\mathbb{Q}$-curve in the sense of [**21**]. Of course, this equation is not a good one at the primes of H above lying above 2 and 3, but it has nevertheless the rather striking property that its discriminant is equal to 1. In fact, we shall see later that $A^{(-\beta)}$ has good reduction outside the set of primes of H lying above $\mathfrak{p}$ for all primes $q \equiv 7 \bmod 8$ (see Corollary 7.12). More generally, we point out that, for any imaginary quadratic field K, equation (1.2) defines an elliptic curve with complex multiplication by the full ring of integers of this imaginary quadratic field, which is defined over an extension of degree at most 6 of the Hilbert class field of K, and which has good reduction outside the set of primes dividing 2 and 3. In fact, classical results due to Weber and Sohngen (see [**2**]) show that the curve (1.2) is defined over H itself whenever the discriminant of K is prime to 6. We hope to study systematically the arithmetic properties of this elliptic curve in a subsequent paper. In the present case, when $K = \mathbb{Q}(\sqrt{-q})$ with q any prime $\equiv 7 \bmod 8$, we prove the following two results about the arithmetic of our curve (1.2). By class field theory, there is a unique $\mathbb{Z}_2$-extension K_∞/K which is unramified outside $\mathfrak{p}$, and, for each integer $n \geqslant 0$, we define K_n to be the unique intermediate field with $[K_n : K] = 2^n$. Put $H_n = HK_n$, and note that $[H_n : H] = 2^n$, since the class number of K is odd. Write $L(A^{(-\beta)}/H_n, s)$ for the complex L-series of $A^{(-\beta)}/H_n$.

THEOREM 1.5. *For all primes $q \equiv 7 \bmod 8$, we have $L(A^{(-\beta)}/H_n, 1) \neq 0$ for all $n \geqslant 0$.*

COROLLARY 1.6. *For all primes $q \equiv 7 \bmod 8$, $Ш(A^{(-\beta)}/H)$ is finite, and also $A^{(-\beta)}(H_n)$ is finite for all $n \geqslant 0$.*

We now explain a curious consequence of this theorem. Write $\mathfrak{M}_K$ for the set of all non-zero integers M in $\mathcal{O}_K$, which are prime to q, satisfy $M \equiv 1 \bmod 4$, and are not squares in K. For each $M \in \mathfrak{M}_K$, define

$$E = A^{(M)} \tag{1.3}$$

to be the twist of A by the extension $H(\sqrt{M})/H$, which is non-trivial because the class number of K is odd. Define

$$\mathcal{F} = H(E_{\mathfrak{p}^2}),\ \mathcal{F}_n = \mathcal{F}H_n = H(E_{\mathfrak{p}^{n+2}}).$$

Write g_{E/H_n} and $g_{E/\mathcal{F}_n}$ for the respective ranks of the Mordell–Weil groups of E/H_n and $E/\mathcal{F}_n$, and let $L(E/H_n, s)$ and $L(E/\mathcal{F}_n, s)$ denote their respective complex L-series.

THEOREM 1.7. *Assume that $q \equiv 7 \bmod 8$, and that $M \in \mathfrak{M}_K$. Then, for all $n \geqslant 0$, we have that $g_{E/H_n} = g_{E/\mathcal{F}_n}$, and $\operatorname{ord}_{s=1} L(E/H_n, s) = \operatorname{ord}_{s=1} L(E/\mathcal{F}_n, s)$.*

We remark that Theorems 1.1 and 1.7 do not seem to have been known before even in the special case $q = 7$, when $A = X_0(49)$ (see, however, the remarks at the end of [**5**]). Of course, we have no way at present of hoping to prove that the four integers $g_{E/H_n}, g_{E/\mathcal{F}_n}, \operatorname{ord}_{s=1} L(E/H_n, s)$, and $\operatorname{ord}_{s=1} L(E/\mathcal{F}_n, s)$ are all equal, as is predicted by the conjecture of Birch and Swinnerton-Dyer.

Finally, we make a conjecture about the elliptic curve (1.2) in the case when $K = \mathbb{Q}(\sqrt{-q})$, with q now a prime satisfying $q \equiv 3 \bmod 8$, so that 2 is inert in K. Then, provided we now take the square root of $j(\mathcal{O}_K) - (12)^3$ lying in the lower half complex plane, and assume $q > 3$, the curve (1.2) is still the twist by the quadratic extension $H(\sqrt{-\beta})/H$ of the Gross curve A/H, whose existence is proven in [**21**]. Thus, since A has good reduction outside the set of primes of H above q, and (1.2) has discriminant 1, the curve $A^{(-\beta)}$ will always have good reduction outside the set of primes of H lying above the prime $p = 2$, assuming $q > 3$.

CONJECTURE 1.8. For all primes q with $q \equiv 3 \bmod 8$, we have $L(A^{(-q)}/H, 1) \neq 0$.

However, we hasten to say that, in contrast to the proof of Theorem 1.5 above, we see absolutely no way at present for attacking such a conjecture using Iwasawa theory. Nevertheless, some remarkable numerical evidence in support of this conjecture has been found very recently by Dabrowski, Jedrzejak, and Szymaszkiewicz (see [**15**]), who have shown that $L(A^{(-q)}/H, 1) \neq 0$ for all primes $q \equiv 3 \bmod 8$ with $q \leqslant 10\,163$.

The reader will quickly realize that the novelty of the arguments in the present paper is to show that it turns out to be much simpler to deal with some of the algebraic aspects of the Iwasawa theory of the h-dimensional abelian variety B/K, which is the restriction of scalars from H to K of the elliptic curve A/H, rather than for the elliptic curve A/H itself. This technique has not been exploited widely in the literature, although it is used earlier in [**24**]. The key arguments used in this paper make essential use throughout of the fact that we are working with the prime $p = 2$, notably in the use of Nakayama's lemma and the fact that both K and the whole tower of fields F_n $(n \geqslant 0)$ all have odd class number in § 3, and in Zhao's induction method in § 9. We establish all of our analytic results for the Iwasawa theory in §§ 4–7 by employing the Euler system of elliptic units as defined in the Appendix of [**8**], showing that this Euler system works beautifully even for the prime $p = 2$. Finally, § 9 of the paper explains how to use Zhao's induction method for the abelian variety B/K.

In further joint work in preparation with Kezuka and Tian [**10**], we hope to use Iwasawa theory to prove the exact Birch–Swinnerton-Dyer formula for the order of the Tate–Shafarevich group of all the elliptic curves with complex multiplication appearing in Theorems 1.3 and 1.5. The two papers of Dabrowski, Jedrzejak, and Szymaszkiewicz [**15**] and [**16**] contain some remarkable tables of numerical values of the orders of these Tate–Shafarevich groups, assuming the exact Birch–Swinnerton-Dyer formula for their order.

The present paper grew out of [**5**], which discussed only the case $q = 7$. We would like to thank the organizers of the conference 'Iwasawa 2017' held at Tokyo University in July 2017 for providing us with an excellent opportunity to initially discuss the ideas developed here. The first author would also like to thank Tsinghua University and the Morningside Center of the Chinese Academy of Sciences for generous hospitality while much of the subsequent detailed work was being developed. Finally, we thank Zhibin Liang for making some numerical computations related to Theorem 8.2, and Jianing Li for informing us of his extremely ingenious elementary proof of Corollary 8.3.

2. *Notation and preliminaries*

We shall use the following notation throughout the rest of this paper. We write

$$B = \mathrm{Res}_{H/K}(A), \tag{2.1}$$

for the abelian variety which is obtained from A by restriction of scalars from H to K (see [**21**, § 15]). We define

$$\mathscr{B} = End_K(B), \ \mathscr{T} = \mathscr{B} \otimes \mathbb{Q}.$$

Then $\mathscr{T}$ is a CM field of degree h of K. Let

$$\psi_{A/H} : \mathbb{A}_H^\times \to K^\times, \ \phi : \mathbb{A}_K^\times \to \mathscr{T}^\times$$

be the Serre–Tate characters (see [**30**, Theorem 10]) attached to A/H and B/K, respectively, where $\mathbb{A}_H^\times$ (respectively, $\mathbb{A}_K^\times$) denotes the idele group of H (respectively of K). Then we have

$$\psi_{A/H} = \phi \circ N_{H/K}$$

where $N_{H/K}$ is the norm map from the idele group of H to the idele group of K. The conductor of ϕ is equal to $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$. For a more detailed discussion of the following facts, see [3, § 1], and [21, § 13]. The endomorphism ring $\mathscr{B}$ is generated over $\mathcal{O}_K$ by the values $\phi(\mathfrak{c})$ for $\mathfrak{c}$ running over all integral ideals of K prime to $\mathfrak{q}$, and has discriminant $h^h\mathcal{O}_K$ as an $\mathcal{O}_K$-module. Thus $\mathscr{B}$ is an order in the field $\mathscr{T}$, which is not necessarily maximal. However, it is always maximal when localized away from h. Also, the field $\mathscr{T}$ contains only 2 roots of unity, and we have $H \cap \mathscr{T} = K$. We fix any embedding of $\mathscr{T}$ in $\mathbb{C}$

$$i : \mathscr{T} \to \mathbb{C}. \tag{2.2}$$

which extends our given embedding of K in $\mathbb{C}$. When there is no danger of confusion, we will omit the embedding i from the notation.

LEMMA 2.1. *The prime* 2 *is unramified in the field* $\mathscr{T}$*, and there is a prime* $\mathfrak{P}$ *of* $\mathscr{T}$ *above* $\mathfrak{p}$ *with residue field of order* 2.

Proof. Since the class number h of K is odd, it follows from the above remarks that 2 will be unramified in the field $\mathscr{T}$. Furthermore, the finitely generated abelian group $A(H) = B(K)$ is a module for the algebra $\mathscr{B}$, and the torsion subgroup of this abelian group is $\mathcal{O}_K/2\mathcal{O}_K$ (see [21, § 13]). This action of $\mathscr{B}$ stabilizes the torsion, and thus gives an $\mathcal{O}_K$-algebra surjection

$$\mathscr{B} \to \mathcal{O}_K/2\mathcal{O}_K.$$

The kernel of this homomorphism is the product of two conjugate primes $\mathfrak{P}, \mathfrak{P}^*$ in $\mathscr{T}$, and $\mathfrak{P}$ has the desired property. □

Gross [22] has proven the existence of a global minimal Weierstrass equation for A over H, and we fix one such minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.3}$$

whose coefficients are algebraic integers in H. Since $H = K(j(\mathcal{O}_K))$, our fixed embedding of K in $\mathbb{C}$ induces an embedding of H into $\mathbb{C}$. The Néron differential $\omega = dx/(2y + a_1x + a_3)$ then has a complex period lattice of the form $\mathcal{L} = \Omega_\infty(A)\mathcal{O}_K$, where $\Omega_\infty(A)$ is uniquely determined up to sign. Further, we have the Weierstrass isomorphism $\mathcal{W}(z, \mathcal{L}) : \mathbb{C}/\mathcal{L} \simeq A(\mathbb{C})$ given by

$$\mathcal{W}(z, \mathcal{L}) = (\wp(z, \mathcal{L}) - b_2/12, \tfrac{1}{2}(\wp'(z, \mathcal{L}) - a_1(\wp(z, \mathcal{L}) - b_2/12) - a_3), \tag{2.4}$$

where $b_2 = a_1^2 + 4a_2$, and $\wp(z, \mathcal{L})$ is the classical Weierstrass $\wp$-function of the lattice $\mathcal{L}$. Put $\mathfrak{G} = \mathrm{Gal}(H/K)$. If $\mathfrak{a}$ is an integral ideal of K with $(\mathfrak{a}, \mathfrak{q}) = 1$, we write $\sigma_\mathfrak{a}$ for the Artin symbol of $\mathfrak{a}$ in $\mathfrak{G}$. Given such an ideal $\mathfrak{a}$, $A^\mathfrak{a}$ will denote the elliptic curve over H which is obtained by applying $\sigma_\mathfrak{a}$ to the coefficients of equation (2.3) for A. We write $(x_\mathfrak{a}, y_\mathfrak{a})$ for a generic point on $A^\mathfrak{a}$. The endomorphism $\phi(\mathfrak{a})$ of the abelian variety B defines a canonical H-isogeny

$$\eta_A(\mathfrak{a}) : A \to A^\mathfrak{a}, \tag{2.5}$$

with kernel precisely the Galois module $A_\mathfrak{a}$ of $\mathfrak{a}$-division points on A. Then, as is explained in [19, § 4], the pull back by $\eta_A(\mathfrak{a})$ of the Néron differential $\omega_\mathfrak{a}$ on $A^\mathfrak{a}$ must be of the form $\xi(\mathfrak{a})\omega$, where $\xi(\mathfrak{a})$ is a uniquely determined non-zero element of H. Further, always with our fixed embedding of H into $\mathbb{C}$, the complex period lattice $\mathcal{L}_\mathfrak{a}$ of $\omega_\mathfrak{a}$ is then equal to $\xi(\mathfrak{a})\Omega_\infty(A)\mathfrak{a}^{-1}$, with Weierstrass isomorphism $\mathcal{W}(z, \mathcal{L}_\mathfrak{a}) : \mathbb{C}/\mathcal{L}_\mathfrak{a} \simeq A^\mathfrak{a}(\mathbb{C})$.

For $\alpha \in \mathscr{B}$, let B_α to be the kernel of the endomorphism α on $B(\bar{K})$, and, for each integer $n \geqslant 1$, define $B_{\mathfrak{P}^n} = \cap_{\alpha \in \mathfrak{P}^n} B_\alpha$. We shall mainly be studying the Iwasawa theory of B over the tower of fields F_∞/K, where

$$F = K(B_{\mathfrak{P}^2}),\ F_n = K(B_{\mathfrak{P}^{n+2}})\ (n \geqslant 0),\ F_\infty = K(B_{\mathfrak{P}^\infty}), \tag{2.6}$$

and $B_{\mathfrak{P}^\infty} = \cup_{n \geqslant 1} B_{\mathfrak{P}^n}$. Lurking in the background, we will also consider the Iwasawa theory of A over the tower of fields

$$\mathfrak{F} = H(A_{\mathfrak{p}^2}),\ \mathfrak{F}_n = H(A_{\mathfrak{p}^{n+2}})\ (n \geqslant 0),\ \mathfrak{F}_\infty = H(A_{\mathfrak{p}^\infty}). \tag{2.7}$$

Moreover, as in the Introduction, let K_∞ be the unique $\mathbb{Z}_2$-extension of K which is unramified outside $\mathfrak{p}$, and write K_n for the unique intermediate field with $[K_n : K] = 2^n$. Put

$$G = \mathrm{Gal}(F_\infty/K),\ \ \mathcal{G} = \mathrm{Gal}(\mathfrak{F}_\infty/H),$$

and let

$$\rho_{\mathfrak{P}} : G \to \mathbb{Z}_2^\times, \rho_{\mathfrak{p}} : \mathcal{G} \to \mathbb{Z}_2^\times \tag{2.8}$$

be the characters giving the action of these two Galois groups on $B_{\mathfrak{P}^\infty}$ and $A_{\mathfrak{p}^\infty}$, respectively. In fact, for reasons which we explain in the next paragraph, both of these characters are isomorphisms. We write $\mathscr{I}$ for the ring of integers of the completion of the maximal unramified extension of $K_{\mathfrak{p}}$. For any p-adic Lie group $\mathfrak{H}$, $\Lambda_{\mathscr{I}}(\mathfrak{H})$ will denote the Iwasawa algebra of $\mathfrak{H}$ with coefficients in $\mathscr{I}$.

Throughout the paper, w will denote a place of H lying above $\mathfrak{p}$. We write H_w for the completion of H at w, and $\mathcal{O}_{H,w}$ for the ring of integers of H_w. For $\mathfrak{c}$ any integral ideal of K, with $(\mathfrak{c}, \mathfrak{q}) = 1$, let $\widehat{A^{\mathfrak{c}}_w}$ be the formal group of $A^{\mathfrak{c}}$ at w. It is a formal group defined over $\mathcal{O}_{H,w}$ with local parameter $t_{\mathfrak{c},w} = -x_{\mathfrak{c}}/y_{\mathfrak{c}}$.

LEMMA 2.2. *For each integral ideal $\mathfrak{c}$ of K prime to $\mathfrak{q}$, $\widehat{A^{\mathfrak{c}}_w}$ is a relative Lubin–Tate formal group in the sense of* [17] *for the unramified extension $H_w/K_{\mathfrak{p}}$.*

Proof. The canonical isogeny $\eta_{A^{\mathfrak{c}}}(\mathfrak{p}) : A^{\mathfrak{c}} \to A^{\mathfrak{cp}}$ induces a map of formal groups defined over $\mathcal{O}_{H,w}$

$$\widehat{\eta_{A^{\mathfrak{c}},\mathfrak{p},w}} : \widehat{A^{\mathfrak{c}}_w} \to \widehat{A^{\mathfrak{cp}}_w}, \tag{2.9}$$

which can be realized by a formal power series $\widehat{\eta_{A^{\mathfrak{c}},\mathfrak{p},w}}(t_{\mathfrak{c},w})$ lying in $\mathcal{O}_{H,w}[[t_{\mathfrak{c},w}]]$. Moreover, since ϕ is the Serre–Tate character of B, it is not difficult to see that

$$\widehat{\eta_{A^{\mathfrak{c}},\mathfrak{p},w}}(t_{\mathfrak{c},w}) \equiv t^2_{\mathfrak{c},w} \bmod w,\ \ \widehat{\eta_{A^{\mathfrak{c}},\mathfrak{p},w}}(t_{\mathfrak{c},w}) \equiv m_{\mathfrak{c}} t_{\mathfrak{c},w} \bmod t^2_{\mathfrak{c},w}\mathcal{O}_{H,w}[[t_{\mathfrak{c},w}]], \tag{2.10}$$

where $N_{H_w/K_{\mathfrak{p}}}(m_{\mathfrak{c}})$ has $\mathfrak{p}$-order equal to $[H_w : K_{\mathfrak{p}}]$. These are precisely the conditions required to define a Lubin–Tate formal group relative to $H_w/K_{\mathfrak{p}}$. □

COROLLARY 2.3. *The prime w is totally ramified in the extension $H_w(A_{\mathfrak{p}^\infty})/H_w$, and the Galois group of this extension is isomorphic to $\mathcal{O}_{\mathfrak{p}}^\times$.*

THEOREM 2.4. *The abelian variety B has good reduction everywhere over the field $F = K(B_{\mathfrak{P}^2})$, and the elliptic curve A has good reduction everywhere over the field $\mathfrak{F} = H(A_{\mathfrak{p}^2})$.*

Proof. We give the proof for B, and the proof for A is entirely similar. The conductor of ϕ is prime to 2, and thus the abelian variety B has good reduction at the primes of K lying above 2. Let ϕ_F be the Serre–Tate homomorphism attached to B over the field F, so that $\phi_F = \phi \circ N_{F/K}$, where $N_{F/K}$ denotes the norm map from the idele group of F to the idele group of K. Let v be any place of F which does not lie above 2, and let U_v be the group of units of the completion F_v of F at v. As is shown in [30], B will have good reduction at v if and only if $\phi_F(U_v) = 1$. But $\phi_F(U_v) = \phi(J_{v'})$, where v' denotes the place of K below v, and $J_{v'}$ denotes the image of U_v under the local norm from F_v to $K_{v'}$. Let $\xi_K : \mathbb{A}_K^\times \to G_K^{ab}$, where G_K^{ab} denotes the Galois group of the maximal abelian extension of K, be Artin's global

reciprocity map. Note that $\xi_K(J_{v'})$ fixes F. We write $\nu_{\mathfrak{P}} : G_K^{ab} \to \mathcal{O}_{\mathfrak{p}}^{\times}$ for the character giving the action of G_K^{ab} on $B_{\mathfrak{P}^\infty}$. Now B has potential good reduction everywhere, since the same assertion is true for the elliptic curve A and its conjugate curves over H. Hence, since v' does not lie above 2, by the criterion of Néron–Ogg–Shafarevich, we must have that $\nu_{\mathfrak{P}}(\xi_K(x))$ is a root of unity for each x in the local units at v'. Moreover, by another basic property of the Serre–Tate homomorphism (see [**30**, Theorem 11]), we have $\nu_{\mathfrak{P}}(\xi_K(x)) = \phi(x)$ for every x in the local units at v'. Now assume that x lies in $J_{v'}$, so that $\nu_{\mathfrak{P}}(\xi_K(x))$ must belong to the subgroup $1 + \mathfrak{P}^2$ of $\mathcal{O}_{\mathfrak{p}}^{\times}$. But this subgroup contains no non-trivial roots of unity, whence we must have that $\nu_{\mathfrak{P}}(\xi_K(x)) = 1$, and so $\phi(x) = 1$. Hence B has good reduction everywhere over F, as claimed. □

LEMMA 2.5. *We have strict inclusions $K_\infty \subset F_\infty \subset \mathfrak{F}_\infty$, and $F_\infty = FK_\infty, \mathfrak{F}_\infty = HF_\infty$. Moreover, the two characters (2.8) are both isomorphisms, the prime $\mathfrak{p}$ of K is totally ramified in F_∞, and all primes of H above $\mathfrak{p}$ are totally ramified in $\mathfrak{F}_\infty$.*

Proof. We first remark that the classical theory of complex multiplication shows that $K_\infty \subset \mathfrak{F}_\infty$. Let w be any prime of H above $\mathfrak{p}$. Then, by Lemma 2.2, w is totally ramified in $\mathfrak{F}_\infty$, and the character $\rho_{\mathfrak{p}}$ is an isomorphism. Thus we must have $\mathfrak{F}_\infty = \mathfrak{F}K_\infty$. Also, we must have $F_\infty \subset \mathfrak{F}_\infty$ since B is isomorphic over H to the product of the h curves conjugate to A under the action of $\mathrm{Gal}(H/K)$. It then follows that $\mathfrak{p}$ must be totally ramified in F_∞. Furthermore, since B has good reduction everywhere over F, we have $F \neq K$, and thus $\rho_{\mathfrak{P}}$ must be an isomorphism. This completes the proof. □

If $\mathfrak{b}$ is any ideal of K prime to $\mathfrak{pq}$, we shall write $\tau_{\mathfrak{b}}$ for the Artin symbol of $\mathfrak{b}$ in $\mathrm{Gal}(\mathfrak{F}_\infty/K)$. Note that, since ϕ is the Serre–Tate character of B, the Artin symbol $\tau_{\mathfrak{b}}$ will fix the field F_n if and only if

$$\phi(\mathfrak{b}) \equiv 1 \mod \mathfrak{P}^{n+2}. \tag{2.11}$$

For each $n \geqslant 0$, we fix a set $\mathfrak{C}_n$ of integral ideals of K, prime to $\mathfrak{pq}$ such that

$$\mathrm{Gal}(\mathfrak{F}_n/F_n) = \{\tau_{\mathfrak{c}}|\mathfrak{F}_n \ : \mathfrak{c} \in \mathfrak{C}_n\}. \tag{2.12}$$

Thus the elements of $\mathfrak{C}_n$ satisfy (2.11), and also give a complete set of representatives of the ideal class group of K since the restriction map from $\mathrm{Gal}(\mathfrak{F}_n/F_n)$ to $\mathrm{Gal}(H/K)$ is an isomorphism.

The restriction map defines an isomorphism from $\mathrm{Gal}(\mathfrak{F}_\infty/F_\infty)$ to $\mathrm{Gal}(H/K)$, and we define δ to be the unique element of $\mathrm{Gal}(\mathfrak{F}_\infty/F_\infty)$ whose restriction to H is the Artin symbol $\sigma_{\mathfrak{p}}$ of $\mathfrak{p}$. Finally, we fix a set $\{V_n \ : \ n \geqslant 0\}$ of primitive $\mathfrak{p}^{n+2}$-division points on A, which are compatible in the sense that

$$\eta_A(\mathfrak{p})(V_{n+1}) = V_n^{\delta} \ \ (n \geqslant 0). \tag{2.13}$$

Note that V_n^{δ} is a primitive $\mathfrak{p}^{n+2}$-division point on $A^{\mathfrak{p}}$.

3. *Iwasawa theory for the abelian variety B over the field $F_\infty = K(B_{\mathfrak{P}^\infty})$*

The aim of this section is to use some very elementary arguments from Iwasawa theory to study descent theory on B over $F_\infty = K(B_{\mathfrak{P}^\infty})$. Note that the proof of Theorem 3.1 depends crucially on the fact that $p = 2$. We define $M(F_\infty)$ to be the maximal abelian 2-extension of $F_\infty = K(B_{\mathfrak{P}^\infty})$, which is unramified outside the primes lying above $\mathfrak{p}$, and put

$$X(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty).$$

We recall that we have chosen the sign of $\sqrt{-q}$ so that $\mathrm{ord}_{\mathfrak{p}}(\sqrt{-q} - 1)/2) > 0$.

THEOREM 3.1. *For all primes q with $q \equiv 7 \bmod 8$, $X(F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module of rank at most $2^{k-2}-1$, where $k = ord_{\mathfrak{p}}(\sqrt{-q}-1)$. In particular, $X(F_\infty) = 0$ when $q \equiv 7 \bmod 16$.*

As is explained in more detail at the very end of § 8, the recent ingenious elementary work of Li [**25**] does in fact imply that $X(F_\infty) \neq 0$ for all primes $q \equiv 15 \bmod 16$. We now closely follow the arguments of elementary Iwasawa theory given in [**5**, § 2] to prove Theorem 3.1. Of course, $M(F_\infty)$ is Galois over K by maximality, and thus $G = \mathrm{Gal}(F_\infty/K)$ has the usual natural continuous action of Iwasawa theory on $X(F_\infty)$. We also remark that, since $\rho_{\mathfrak{P}}$ is an isomorphism, the Galois group G is of the form $G = \Delta \times \Gamma$, where Δ is cyclic of order 2 and Γ is isomorphic to $\mathbb{Z}_2$, and all of our arguments will be based on Nakayama's lemma for either of the natural Δ-actions or Γ-actions. Let $\mathfrak{R} = \mathbb{Z}_2[\Delta]$ be the group ring of Δ over $\mathbb{Z}_2$. If V is any $\mathfrak{R}$-module, we write as usual V_Δ for the largest quotient of V on which Δ acts trivially. Similarly, if V is a compact Γ-module which is a $\mathbb{Z}_2$-module, $(V)_\Gamma$ will be the largest quotient of V on which Γ acts trivially.

LEMMA 3.2. *The field K_∞ has no non-trivial abelian 2-extension, which is unramified outside the unique prime of K_∞ above $\mathfrak{p}$.*

Proof. Denote by $M(K_\infty)$ the maximal abelian 2-extension over K_∞ which is unramified outside the unique prime above $\mathfrak{p}$, and let $X(K_\infty)$ be the Galois group $\mathrm{Gal}(M(K_\infty)/K_\infty)$. Since $M(K_\infty)$ is Galois over K by maximality, the Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ acts on it continuously by lifting inner automorphisms. We claim that $(X(K_\infty))_\Gamma = 0$, which will suffice to prove what we want by Nakayama's lemma. Denote by $\mathfrak{J}$ the maximal abelian extension of K in $M(K_\infty)$, so that $\mathrm{Gal}(\mathfrak{J}/K_\infty) = (X(K_\infty))_\Gamma$. Now, since the class number of K is odd, class field theory shows immediately that K_∞ itself is the maximal abelian 2-extension of K which is unramified outside $\mathfrak{p}$. Hence $\mathfrak{J} = K_\infty$, and the proof is complete. □

LEMMA 3.3. *Let r_q denote the number of primes of K_∞ lying above the prime $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$ of K. Then $r_q = 2^{k-2}$, where $k = ord_{\mathfrak{p}}(\sqrt{-q}-1)$.*

Proof. It follows from the definition of k that $\sqrt{-q} \in 1 + \mathfrak{p}^k$ but $\sqrt{-q} \notin 1 + \mathfrak{p}^{k+1}$, where $k \geqslant 2$. Noting that K_n is the 2-part of the ray class field of K modulo $\mathfrak{p}^{n+2}$ for all $n \geqslant 0$, we then conclude easily from class field theory that $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$ splits completely in the extension K_{k-2}, and that each prime of K_{k-2} above $\mathfrak{q}$ is inert in K_∞. Thus there are precisely r_q primes of K_∞ above $\mathfrak{q}$, and the proof is complete. □

LEMMA 3.4. *We have $(X(F_\infty))_\Delta$ is an $\mathbb{F}_2$-vector space of dimension at most $r_q - 1$, where $\mathbb{F}_2$ denotes the field with 2 elements.*

Proof. By the definition of the Δ action, we have $\mathrm{Gal}(\mathfrak{I}/F_\infty) = (X(F_\infty))_\Delta$, where $\mathfrak{I}$ is the maximal abelian extension of K_∞ contained in $M(F_\infty)$. But the only primes of K_∞ which ramify in $\mathfrak{I}$ are the unique prime above $\mathfrak{p}$, and the r_q primes above $\mathfrak{q}$. Moreover, the ramification index of each of these primes above $\mathfrak{q}$ in $\mathfrak{I}$ is precisely 2, because this is the ramification index of $\mathfrak{q}$ in F. Let $\mathcal{D}$ denote the subgroup of $\mathrm{Gal}(\mathfrak{I}/K_\infty)$ generated by the inertial subgroups of these primes above $\mathfrak{q}$. Thus $\mathcal{D}$ is a vector space of dimension at most r_q over $\mathbb{F}_2$. Now the fixed field of $\mathcal{D}$ is an abelian 2-extension of K_∞ unramified outside $\mathfrak{p}$. Thus, by Lemma 3.2, this fixed field must be equal to K_∞. Hence $\mathcal{D} = \mathrm{Gal}(\mathfrak{I}/K_\infty)$, and the assertion of the lemma follows because $[F_\infty : K_\infty] = 2$. □

COROLLARY 3.5. *$X(F_\infty)$ is a finitely generated $\mathfrak{R}$-module, which is generated by at most $2^{k-2}-1$ elements over $\mathfrak{R}$. In particular, $X(F_\infty))$ is a finitely generated $\mathbb{Z}_2$-module.*

Proof. As $X(F_\infty)$ is a compact $\mathfrak{R}$-module, the corollary follows immediately from Lemma 3.4 and the Nakayama lemma. □

LEMMA 3.6. *$X(F_\infty)$ is a free $\mathbb{Z}_2$-module, and $X(F_\infty)^\Delta = 0$.*

Proof. We have the exact sequence of finitely generated $\mathbb{Z}_2$-modules

$$0 \to (X(F_\infty))^\Delta \to X(F_\infty) \to X(F_\infty) \to (X(F_\infty))_\Delta \to 0,$$

where the middle map is given by multiplication $1-\epsilon$, where ϵ denotes the non-trivial element of Δ. Since $(X(F_\infty))_\Delta$ is finite by Lemma 3.4, it follows that $X(F_\infty)^\Delta$ is also finite. But $X(F_\infty)^\Delta$ is also a Γ-module, whence by the theorem of Greenberg [**20**, p. 94], asserting that $X(F_\infty)$ has no non-zero finite Γ-submodule in our case even when $p=2$, we conclude that $(X(F_\infty))^\Delta = 0$, and also that the torsion subgroup of $X(F_\infty)$ must be zero. This completes the proof. □

We omit the proof (see [**5**, Lemma 2.8]) of the following simple algebraic lemma, whose proof was pointed out to one of us by Romyar Sharifi.

LEMMA 3.7. *Let Y be a free $\mathbb{Z}_2$-module of finite rank, which is also a Δ-module, and assume $(Y)_\Delta = (\mathbb{Z}/2\mathbb{Z})^r (r \geqslant 0)$. Then Y is a free $\mathbb{Z}_2$-module of rank r.*

Combining Corollary 3.5, and Lemmas 3.6, and 3.7, the proof of Theorem 3.1 is complete.

Remarkably, the following result is valid for all primes q with $q \equiv 7 \bmod 8$.

THEOREM 3.8. *For all primes q with $q \equiv 7 \bmod 8$, the field $F_n = K(B_{\mathfrak{P}^{n+2}})$ has odd class number for all $n \geqslant 0$, and F_∞ has no unramified abelian 2-extension.*

Proof. We first show that F has odd class number. Let $L(F)$ be the 2-Hilbert class field of F, and put $Y(F) = \mathrm{Gal}(L(F)/F)$. By maximality, $L(F)$ is Galois over K, and so Δ acts on $Y(F)$ in the usual fashion. Thus $Y(F)_\Delta = \mathrm{Gal}(J/F)$, where J is the maximal abelian extension of K contained in $L(F)$. Now the only primes of K which are ramified in J are $\mathfrak{p}$ and $\mathfrak{q}$. Let Φ be the inertial subgroup of $\mathfrak{q}$ in $\mathrm{Gal}(J/K)$. Then the fixed field J^Φ of Φ must be an abelian 2-extension of K which is unramified outside of $\mathfrak{p}$. But, since K has odd class number, the only abelian 2-extensions of K unramified outside of $\mathfrak{p}$ are the fields $K_n (n \geqslant 0)$, and so we must have $J^\Phi = K_m$ for some m. But then it follows that $K_m F \subset J$, and so the extension $K_m F/F$ is unramified. But the unique prime above $\mathfrak{p}$ is totally ramified in the extension $K_m F/F$. Thus we must have $K_m \subset F$. However, $K_m \neq F$ because $\mathfrak{q}$ is ramified in F, and so we conclude that $m = 0$. Hence we have shown that K is the fixed field of Φ, and so $\mathrm{Gal}(J/K) = \Phi$. But $\mathfrak{q}$ has ramification index 2 in the extension J/K, so that Φ has order 2, whence also $\mathrm{Gal}(J/K)$ has order 2. It follows that necessarily $J = F$, and so $Y(F)_\Delta = 0$. But then by Nakayama's lemma, we must have $Y(F) = 0$, proving that F has odd class number.

Now let $L(F_\infty)$ be the maximal unramified abelian 2-extension of F_∞, and put $Y(F_\infty) = \mathrm{Gal}(L(F_\infty)/F_\infty)$. Recall that $\Gamma = \mathrm{Gal}(F_\infty/F)$. Now the $\mathbb{Z}_2$-extension F_∞/F is totally ramified at the unique prime of F above $\mathfrak{p}$, and no other prime of F is ramified in it. A classical argument in Iwasawa theory then proves that $Y(F_\infty)_\Gamma \simeq \mathrm{Gal}(L(F)/F)$, where again $L(F)$ denotes the 2-Hilbert class field of F. But we have just shown that $L(F) = F$. Hence $Y(F_\infty)_\Gamma = 0$, and so by the topological Nakayama's lemma, we must have $Y(F_\infty) = 0$. But, if we write $L(F_n)$ for the 2-Hilbert class field of F_n for any $n \geqslant 0$, the same classical argument in Iwasawa theory

shows that $Y(F_\infty)_{\Gamma_n} \simeq \mathrm{Gal}(L(F_n)/F_n)$, where Γ_n denotes the unique closed subgroup of Γ of index 2^n. Hence $L(F_n) = F_n$, and so F_n has odd class number for all $n \geqslant 0$. This completes the proof. □

The above arguments make essential use of the fact that we are working with Galois groups. However, for the arithmetic applications, it is important that we translate all into assertions about Selmer groups, as is done in [5] in the special case $q = 7$. We make use of the standard notation for the Galois cohomology of Galois modules and abelian varieties. Recall that $\mathscr{B}$ is the ring of K-endomorphisms of the abelian variety B. We fix any non-zero element π of $\mathscr{B}$ such that the ideal factorization of π in the ring of integers of $\mathscr{T}$ is $\mathfrak{P}^r$ for some integer $r \geqslant 1$. Now let L be any algebraic extension of K. As usual, we define, for each integer $n \geqslant 1$, the Selmer group $\mathrm{Sel}_{\pi^n}(B/L)$ by the exact sequence

$$\mathrm{Sel}_{\pi^n}(B/L) = \mathrm{Ker}\left(H^1(L, B_{\pi^n}) \to \prod_v H^1(L_v, B)_{\pi^n} \right),$$

where v runs over all finite places of L, and L_v is the compositum of the completions at v of all finite extensions of K contained in L. Passing to the inductive limit over all $n \geqslant 1$, and noting that $B_{\pi^\infty} = B_{\mathfrak{P}^\infty}$, we then define the Selmer group $\mathrm{Sel}_{\mathfrak{P}^\infty}(B/L)$ to be the inductive limit of the Selmer groups $\mathrm{Sel}_{\pi^n}(B/L)$, so that we have

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B/L) = \mathrm{Ker}\left(H^1(L, B_{\mathfrak{P}^\infty}) \to \prod_v H^1(L_v, B)(\mathfrak{P}) \right);$$

here, for any $\mathscr{B}$-module V, we write $V(\mathfrak{P})$ for the submodule of elements which are annihilated by some power of π. In an entirely similar manner, the modified Selmer group $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/L)$ is defined by

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/L) = \mathrm{Ker}\left(H^1(L, B_{\mathfrak{P}^\infty}) \to \prod_{v \nmid \mathfrak{p}} H^1(L_v, B)(\mathfrak{P}) \right),$$

where now the product is taken over all primes v of L which do not lie above the prime $\mathfrak{p}$ of K.

THEOREM 3.9. *We have*

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Hom}(X(F_\infty), B_{\mathfrak{P}^\infty}).$$

Proof. Since B has good reduction everywhere over F, the G_F-module $B_{\mathfrak{P}^\infty}$ is unramified outside the set of primes of F lying above $\mathfrak{p}$. Combining this with the fact that $B_{\mathfrak{P}^\infty}$ is fixed by $\mathrm{Gal}(\bar{F}/F_\infty)$, an entirely similar argument to that given in the proof of [7, Theorem 12] shows that

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Hom}(X(F_\infty), B_{\mathfrak{P}^\infty}).$$

Hence the assertion of the theorem will follow once we have shown that, for the unique place v of F_∞ above $\mathfrak{p}$, we have

$$H^1(F_{\infty,v}, B)(\mathfrak{P}) = 0. \tag{3.1}$$

Since F_∞/K is totally ramified at the unique prime above $\mathfrak{p}$, it follows that the residue field of v restricted to F_n is always equal to $k_v = \mathbb{Z}/2\mathbb{Z}$. Let B' denote the dual abelian variety of B over K, so that B' also has good reduction everywhere over F. We write $\mathfrak{B}'_v$ for the reduction of B' modulo v. Fix at first the integer $n \geqslant 1$. Then Tate local duality at v shows that, for all integers $m \geqslant 1$, $H^1(F_{n,v}, B)_{\pi^n}$ is dual to $B'(F_{n,v})/\pi^{*m} B'(F_{n,v})$, where π^* denotes the complex

conjugate of π for the CM field $\mathscr{T}$. Now v lies above $\mathfrak{p}$, and so π^{*m} is an automorphism of the formal group of B' at v, whence

$$B'(F_{n,v})/\pi^{*m}B'(F_{n,v}) = \mathfrak{B}'_v(k_v)/\pi^{*m}\mathfrak{B}'_v(k_v).$$

Passing to the inductive limit, we conclude that $H^1(F_{n,v}, B)(\mathfrak{P})$ is dual to $\mathfrak{B}'_v(k_v)(\mathfrak{P}^*)$, and so $H^1(F_{\infty,v}, B)(\mathfrak{P})$ will be dual to the projective limit of the $\mathfrak{B}'_v(k_v)(\mathfrak{P}^*)$ with respect to the norm maps up the tower F_∞/F. But the Galois group of F_∞/F acts trivially on the finite group $\mathfrak{B}'_v(k_v)(\mathfrak{P}^*)$, and so the projective limit of these groups with respect to the norm map is clearly zero. Thus completes the proof of (3.1) and the theorem. □

PROPOSITION 3.10. *Recalling that* $\Delta = \mathrm{Gal}(F_\infty/K_\infty)$, *we have*

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^\Delta.$$

Proof. As before, let ϵ be the non-trivial element of Δ, so that ϵ acts on $B_{\mathfrak{P}^\infty}$ by -1. Thus, if f belongs to $\mathrm{Hom}(X(F_\infty), B_{\mathfrak{P}^\infty})$, we have $(\epsilon f)(x) = -f(\epsilon x)$ for all x in $X(F_\infty)$. Hence

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^\Delta = \mathrm{Hom}(X(F_\infty)/(1+\epsilon)X(F_\infty), B_{\mathfrak{P}^\infty}).$$

But $(1+\epsilon)X(F_\infty) \subset X(F_\infty)^\Delta$, and this latter group is zero by Lemma 3.6, whence the assertion of the proposition follows. □

PROPOSITION 3.11. *For all* $n \geqslant 0$, *the restriction map yields an isomorphism*

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_n) \simeq \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^{\Gamma_n},$$

where $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$.

Proof. By the definition of the Selmer group, the restriction maps gives rise to the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_n) & \longrightarrow & H^1(F_n, B_{\mathfrak{P}^\infty}) & \longrightarrow & \prod_{v\nmid\mathfrak{p}} H^1(F_{n,v}, B)(\mathfrak{P}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^{\Gamma_n} & \longrightarrow & H^1(F_\infty, B_{\mathfrak{P}^\infty})^{\Gamma_n} & \longrightarrow & \Big(\prod_{w\nmid\mathfrak{p}} H^1(F_{\infty,w}, B)(\mathfrak{P})\Big)^{\Gamma_n}.
\end{array}$$

Now the middle vertical map is an isomorphism. Indeed $H^2(\Gamma_n, B_{\mathfrak{P}^\infty}) = 0$ because Γ_n has 2-cohomological dimension equal to 1, and a well-known argument (see the proof of [**5**, Lemma 2.11]) shows that also $H^1(\Gamma_n, B_{\mathfrak{P}^\infty}) = 0$. Moreover, the right vertical map is injective because B has good reduction at all primes v, and the extension $F_{\infty,w}/F_{n,v}$ is unramified when w does not lie above the prime $\mathfrak{p}$ of K. The assertion of the lemma now follows. □

THEOREM 3.12. *For all* $n \geqslant 0$, *we have* $\mathrm{Rank}_{\mathbb{Z}}(B(F_n)) = \mathrm{Rank}_{\mathbb{Z}}(B(K_n))$, *and the* $\mathbb{Z}_2$*-corank of* $Ш(B/F_n)(\mathfrak{P})$ *is equal to the* $\mathbb{Z}_2$*-corank of* $Ш(B/K_n)(\mathfrak{P})$, *for all* $n \geqslant 0$.

Proof. Note first that it follows immediately from Propositions 3.10 and 3.11 that, for all $n \geqslant 0$, we have

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_n)^\Delta = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_n). \tag{3.2}$$

Now since Δ is of order 2, one sees easily that the kernel and cokernel of the restriction map from $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/K_n)$ to $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_n)^\Delta$ are annihilated by 2, and so it follows from (3.2) that, for all $n \geqslant 0$, we have

$$\mathbb{Z}_2 - \mathrm{corank\ of\ Sel}'_{\mathfrak{P}^\infty}(B/K_n) = \mathbb{Z}_2 - \mathrm{corank\ of\ Sel}'_{\mathfrak{P}^\infty}(B/F_n). \tag{3.3}$$

Define the modified Shafarevich–Tate group via the exactness of the sequence

$$0 \to Ш'(B/K_n) \to H^1(K_n, B) \to \prod_{v \nmid \mathfrak{p}} H^1(K_{n,v}, B),$$

where v runs over all the finite places of K_n distinct from $\mathfrak{p}$. Note that we then have the exact sequence

$$0 \to B(K_n) \otimes_{\mathscr{B}} (\mathscr{T}_{\mathfrak{P}}/\mathscr{B}_{\mathfrak{P}}) \to \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/K_n) \to Ш'(B/K_n)(\mathfrak{P}) \to 0. \tag{3.4}$$

We have an entirely similar exact sequence for the field F_n. Denote by g_{K_n}, t_{K_n} the $\mathbb{Z}_2$-corank of $B(K_n) \otimes_{\mathscr{B}} (\mathscr{T}_{\mathfrak{P}}/\mathscr{B}_{\mathfrak{P}})$, and of $Ш'(B/K_n)(\mathfrak{P})$, respectively. Define g_{F_n}, t_{F_n} in an entirely analogous fashion for the field F_n. It follows immediately from (3.3) that we have

$$g_{K_n} + t_{K_n} = g_{F_n} + t_{K_n}. \tag{3.5}$$

Note further that $t_{K_n} \leqslant t_{F_n}$ and $g_{K_n} \leqslant g_{F_n}$, because the restriction maps

$$Ш'(B/K_n)(\mathfrak{P}) \to Ш'(B/F_n)(\mathfrak{P}) \text{ and } B(K_n) \otimes_{\mathscr{B}} (\mathscr{T}_{\mathfrak{P}}/\mathscr{B}_{\mathfrak{P}}) \to B(F_n) \otimes_{\mathscr{B}} (\mathscr{T}_{\mathfrak{P}}/\mathscr{B}_{\mathfrak{P}})$$

have finite kernels. Therefore, we conclude from (3.5) that $g_{K_n} = g_{F_n}, t_{K_n} = t_{F_n}$. The first assertion of the theorem now follows easily. For the second assertion, note that we have the exact sequence

$$0 \to Ш(B/K_n)(\mathfrak{P}) \to Ш'(B/K_n)(\mathfrak{P}) \to H^1(K_{n,w}, B)(\mathfrak{P}),$$

where w denotes the unique prime of K_n above $\mathfrak{p}$. But an entirely similar argument with Tate local duality to that used above in the proof of Theorem 3.9 shows that the group on the extreme right of this last exact sequence is finite. Hence t_{K_n} is equal to the $\mathbb{Z}_2$-corank of $Ш(B/K_n)(\mathfrak{P})$. Similarly, we find that t_{F_n} is the $\mathbb{Z}_2$-corank of $Ш(B/F_n)(\mathfrak{P})$, and the proof of the theorem is now complete. □

4. *Ellitpic units for the field* $F_\infty = K(B_{\mathfrak{P}^\infty})$

The aim of the present section is to define, for every $n \geqslant 0$, a suitable group of elliptic units for the field $F_n = K(B_{\mathfrak{P}^{n+2}})$, which we will denote by $C(F_n)$, and to prove the existence of a suitable interpolating power series for them. We use a variant of the method first pioneered in [14].

We first determine the conductors of some of the abelian extensions of K which arise in the rest of the section.

LEMMA 4.1. *Let $\mathfrak{f}$ be any integral ideal of K which is divisible by the conductor $\mathfrak{q}$ of ϕ. Then $H(A_\mathfrak{f})$ is equal to the ray class field of K modulo $\mathfrak{f}$.*

Proof. The classical theory of complex multiplication shows that the ray class field of K modulo $\mathfrak{f}$ is contained in the field $H(A_\mathfrak{f})$. Conversely, suppose that α is an element of K with $\mathrm{ord}_v(\alpha - 1) \geqslant \mathrm{ord}_v(\mathfrak{f})$ for all places v of K dividing $\mathfrak{f}$, and write $(\alpha)_K$ and $(\alpha)_H$ for the respective principal ideals of K and H generated by α. Note that the abelian extension $H(A_\mathfrak{f})/K$ is unramified outside the set of primes of K dividing $\mathfrak{f}$, because all primes of bad reduction for A/H must divide the ideal of H generated by $\mathfrak{f}$. Write m_K for the Artin symbol of $(\alpha)_K$ in $\mathrm{Gal}(H(A_\mathfrak{f})/K)$. We must show that m_K fixes $A_\mathfrak{f}$. To do this, let us consider the Artin symbol m_H of $(\alpha)_H$ for the abelian extension $H(A_\mathfrak{f})/H$. By the definition of the Grossencharacter, the Artin symbol m_H acts on $A_\mathfrak{f}$ by multiplication by the endomorphism

$$\psi_{A/H}((\alpha)_H) = \phi((\alpha)_K^h) = \alpha^h,$$

whence it is clear that m_H fixes $A_{\mathfrak{f}}$. But by the functorality of the Artin symbol, we know that $m_K = m_H^h$, and so it follows that m_K also fixes $A_{\mathfrak{f}}$, as required. □

Recall that $\mathfrak{F}_n = H(A_{\mathfrak{p}^{n+2}}) = HF_n$.

LEMMA 4.2. *For all $n \geqslant 0$, the conductors of the abelian extensions $\mathfrak{F}_n/K$ and F_n/K are both equal to $\mathfrak{f}_n = \mathfrak{q}\mathfrak{p}^{n+2}$.*

Proof. By the previous lemma, we know that $H(A_{\mathfrak{f}_n})$ is equal to the ray class field of K modulo $\mathfrak{f}_n$. But

$$F_n \subset \mathfrak{F}_n \subset H(A_{\mathfrak{f}_n}),$$

and so the conductors of F_n/K and $\mathfrak{F}_n/K$ must both divide $\mathfrak{f}_n$. But K_n/K has conductor equal to $\mathfrak{p}^{n+2}$, since otherwise it would be contained in the field HK_{n-1}, and this is impossible because $\mathfrak{p}$ has ramification index 2^n in K_n. Since $K_n \subset F_n$, it follows that the conductors of F_n/K and $\mathfrak{F}_n/K$ must both be divisible by $\mathfrak{p}^{n+2}$. Moreover, B has good reduction everywhere over the field F_n, and thus its Grossencharacter over this field, which is $\phi \circ N_{F_n/K}$, must have trivial conductor. Hence the conductor $\mathfrak{q}$ of ϕ must divide the conductor of F_n/K. Similarly, A has good reduction everywhere over $\mathfrak{F}_n$, whence again $\mathfrak{q}$ must divided the conductor of $\mathfrak{F}_n/K$. As $\mathfrak{p}$ and $\mathfrak{q}$ are relatively prime, this completes the proof. □

While our aim is to define a group of elliptic units for each of the fields $F_n = K(B_{\mathfrak{P}^{n+2}})$, we need first to discuss the appropriate group of elliptic units for the fields $\mathfrak{F}_n = H(A_{\mathfrak{p}^{n+2}})$. Let us introduce the index set

$$\mathscr{J} = \{\alpha : \alpha \in \mathcal{O}_K, \alpha \neq 0, \pm 1, (\alpha, 6\mathfrak{q}) = 1, \alpha \equiv 1 \bmod \mathfrak{p}^2\}. \tag{4.1}$$

The congruence $\alpha \equiv 1 \bmod \mathfrak{p}^2$ imposed on the elements of $\mathscr{J}$ is not strictly necessary, but we will use it to avoid some technical complications in later arguments. For each $\alpha \in \mathscr{J}$, we defined the rational function $g_{\alpha,A}(P)$ on A/H by

$$g_{\alpha,A}(P) = \prod_V (x(P) - x(V))^{-1}, \tag{4.2}$$

where V runs over any set of representatives of the set of non-zero elements of the Galois module A_α modulo ± 1. Here $P = (x, y)$ is a generic point on (2.3). As is shown by a very elementary argument in the Appendix of [8], there exists a unique non-zero $c_\alpha(A) \in H$ such that the normalized function

$$\mathfrak{g}_{\alpha,A}(P) = c_\alpha(A) g_{\alpha,A}(P) \tag{4.3}$$

satisfies

$$\mathfrak{g}_{\alpha,A}(\beta(P)) = \prod_{W \in A_\beta} \mathfrak{g}_{\alpha,A}(P \oplus W) \tag{4.4}$$

for all non-zero β in $\mathcal{O}_K$ with $(\beta, \alpha) = 1$; here the symbol $\oplus$ denotes the group law on the elliptic curve A. Recalling that $\mathcal{L} = \Omega_\infty(A)\mathcal{O}_K$ is the period lattice of the Néron differential on our generalized Weierstrass equation (2.3) for A/H, we define a primitive $\sqrt{-q}$-division point on A by

$$Q = \mathcal{W}(\Omega_\infty(A)/\sqrt{-q}, \mathcal{L}). \tag{4.5}$$

We then define

$$\mathfrak{R}_{\alpha,A}(P) = \prod_{\tau \in \mathrm{Gal}(H(A_\mathfrak{q})/H)} \mathfrak{g}_{\alpha,A}(P \oplus Q^\tau), \tag{4.6}$$

which is thus a rational function on A with coefficients in H. Plainly $\mathfrak{R}_{\alpha,A}(P)$ depends only on the orbit of Q under the action of $\mathrm{Gal}(H(A_{\mathfrak{q}})/H)$, but note that, in view of Lemma 4.1, this Galois group does not act transitively on the set of all primitive $\mathfrak{q}$-division points of A. It is this which guarantees the all important fact that $\mathfrak{R}_{\alpha,A}(P) \neq \mathfrak{R}_{\alpha,A}(\ominus P)$, where $\ominus$ denotes the subtraction on the elliptic curve. It is also important to define intrinsic analogues of the rational function $\mathfrak{R}_{\alpha,A}(P)$ for every conjugate curve of A/H under the action of the Galois group $\mathfrak{G} = \mathrm{Gal}(H/K)$. Let $Q(\mathfrak{a})$ be the $\mathfrak{q}$-division point on $A^{\mathfrak{a}}$ defined by

$$Q(\mathfrak{a}) = \mathcal{W}(\xi(\mathfrak{a})\Omega_\infty(A)/\sqrt{-q}, \mathcal{L}_{\mathfrak{a}}), \tag{4.7}$$

and define the rational function on $A^{\mathfrak{a}}/H$ by

$$\mathfrak{R}_{\alpha,A^{\mathfrak{a}}}(P) = \prod_{\tau \in \mathrm{Gal}(H(A^{\mathfrak{a}}_{\mathfrak{q}})/H)} \mathfrak{g}_{\alpha,A^{\mathfrak{a}}}(P \oplus Q(\mathfrak{a})^{\tau}). \tag{4.8}$$

Due to Lemma 4.1, the fields $H(A^{\mathfrak{a}}_{\mathfrak{q}})$ are all equal to $H(A_{\mathfrak{q}})$, and then (see [**19**, § 4]) the Artin symbol of $\mathfrak{a}$ in $\mathrm{Gal}(H(A_{\mathfrak{q}})/K)$ maps Q to $Q(\mathfrak{a})$. It follows easily that, whenever $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals of K, which are prime to $\mathfrak{q}$ and lie in the same ideal class, then necessarily $\mathfrak{R}_{\alpha,A^{\mathfrak{a}}}(P) = \mathfrak{R}_{\alpha,A^{\mathfrak{b}}}(P)$.

We first define the group of elliptic units for the field $\mathfrak{F}_n = H(A_{\mathfrak{p}^{n+2}})$ for any integer $n \geqslant 0$. Recall that V_n denotes a primitive $\mathfrak{p}^{n+2}$-division point on the curve A. We then define $C(\mathfrak{F}_n)$ to be the subgroup of $\mathfrak{F}_n^{\times}$ which is generated by all conjugates of $\mathfrak{R}_{\alpha,A}(V_n)$ under the action of the $\mathrm{Gal}(\mathfrak{F}_n/K)$ and all $\alpha \in \mathscr{J}$. We shall show below that the elements of $C(\mathfrak{F}_n)$ are indeed global units. We recall that, if $\mathfrak{c}$ is any integral ideal of K prime to $\mathfrak{pq}$, $\tau_{\mathfrak{c}}$ denotes the Artin symbol of $\mathfrak{c}$ in $\mathrm{Gal}(\mathfrak{F}_\infty/K)$. Since $\tau_{\mathfrak{c}}(A) = A^{\mathfrak{c}}$ and $\tau_c(V_n) = \eta_A(\mathfrak{c})(V_n)$, the action of $\mathrm{Gal}(\mathfrak{F}_n/K)$ on $\mathfrak{R}_{\alpha,A}(V_n)$ is given by the following lemma.

LEMMA 4.3. *For all $n \geqslant 0$, and all integral ideals $\mathfrak{c}$ of K prime to $\mathfrak{pq}$, we have*

$$\tau_{\mathfrak{c}}(\mathfrak{R}_{\alpha,A}(V_n)) = \mathfrak{R}_{\alpha,A^{\mathfrak{c}}}(\eta_A(\mathfrak{c})(V_n)). \tag{4.9}$$

We next discuss the behavior of $C(\mathfrak{F}_n)$ under the norm map $N_{\mathfrak{F}_n/\mathfrak{F}_{n-1}}$ from $\mathfrak{F}_n$ to $\mathfrak{F}_{n-1}$. Now the Artin symbol of $\mathfrak{p}$ cannot be defined in $\mathrm{Gal}(\mathfrak{F}_\infty/K)$. However, we recall that $\mathrm{Gal}(\mathfrak{F}_\infty/F_\infty)$ is isomorphic to $\mathfrak{G}$ under restriction, and δ is the unique element of $\mathrm{Gal}(\mathfrak{F}_\infty/F_\infty)$ whose restriction to $\mathfrak{G}$ is the Artin symbol of $\mathfrak{p}$. Now we have the H-isogeny

$$\eta_A(\mathfrak{p}) : A \to A^{\mathfrak{p}},$$

whose kernel is precisely $A_{\mathfrak{p}}$. Thus $\eta_A(\mathfrak{p})(V_n)$ must be a primitive $\mathfrak{p}^{n+1}$-division point on the curve $A^{\mathfrak{p}}$. On the other hand, it is shown in Theorem 4 of the Appendix of [**8**] that the rational functions $\mathfrak{g}_{\alpha,A}(P)$ behave nicely with respect to isogenies of degree prime to α. Since $(\mathfrak{p}, \alpha) = 1$ because $(\alpha, 6) = 1$, the following lemma then follows easily.

LEMMA 4.4. *We have*

$$\mathfrak{R}_{\alpha,A^{\mathfrak{p}}}(\eta_A(\mathfrak{p})(P)) = \prod_{V \in A_{\mathfrak{p}}} \mathfrak{R}_{\alpha,A}(P \oplus V). \tag{4.10}$$

Now for $n \geqslant 1$, we have $[\mathfrak{F}_n : \mathfrak{F}_{n-1}] = 2$ and the conjugates of V_n under the action of $\mathrm{Gal}(\mathfrak{F}_n/\mathfrak{F}_{n-1})$ are precisely the $V_n \oplus V$ with $V \in A_{\mathfrak{p}}$. Hence we immediately obtain

COROLLARY 4.5. *For all $n \geqslant 1$, we have $N_{\mathfrak{F}_n/\mathfrak{F}_{n-1}}(\mathfrak{R}_{\alpha,A}(V_n)) = \mathfrak{R}_{\alpha,A^{\mathfrak{p}}}(\eta_A(\mathfrak{p})(V_n))$.*

On the other hand, we have already fixed in Section 2 (see (2.13)) the convention that we have chosen the primitive $\mathfrak{p}^{n+1}$-division point V_{n-1} so that $\delta(V_{n-1}) = \eta_A(\mathfrak{p})(V_n)$. Hence the above corollary can be rewritten as giving

$$N_{\mathfrak{F}_n/\mathfrak{F}_{n-1}}(\mathfrak{R}_{\alpha,A}(V_n)) = \delta(\mathfrak{R}_{\alpha,A}(V_{n-1})) \ \ (n \geqslant 1).$$

Hence we immediately obtain the theorem.

THEOREM 4.6. *For all $n \geqslant 1$, we have*

$$N_{\mathfrak{F}_n/\mathfrak{F}_{n-1}}(\delta^{-n}(\mathfrak{R}_{\alpha,A}(V_n))) = \delta^{-(n-1)}(\mathfrak{R}_{\alpha,A}(V_{n-1})).$$

COROLLARY 4.7. *Every element of $C(\mathfrak{F}_n)$ is a global unit.*

Indeed, since every prime of $\mathfrak{F}_n$ which does not lie above $\mathfrak{p}$ is unramified in $\mathfrak{F}_\infty$ and its decomposition group is of finite index, it follows easily from the universal norm property of Theorem 4.6 (see [**8**, Lemma 5]) that the only primes which can possibly divide $\mathfrak{R}_{\alpha,A}(V_n)$ must divide $\mathfrak{p}$. On the other hand, the following classical lemma shows that $\mathfrak{R}_{\alpha,A}(V_n)$ is a unit at each prime w of H above $\mathfrak{p}$ since the power series in Lemma 4.8, in the special case when $\mathfrak{b} = \mathcal{O}_K$, will certainly converge at $t_w(V_n)$ to a unit at w. Let $\mathfrak{b}$ be any integral ideal of K prime to $\mathfrak{q}$. Recall that $P_\mathfrak{b} = (x_\mathfrak{b}, y_\mathfrak{b})$ is the generic point on the equation for $A^\mathfrak{b}$, and that $t_{\mathfrak{b},w} = -x_\mathfrak{b}/y_\mathfrak{b}$ is a parameter for the formal group of $A^\mathfrak{b}$ at w, where w is any prime of H above $\mathfrak{p}$.

LEMMA 4.8. *For each integral ideal $\mathfrak{b}$ of K prime to $\mathfrak{q}$, the $t_{\mathfrak{b},w}$-expansion of $\mathfrak{R}_{\alpha,A^\mathfrak{b}}(P_\mathfrak{b})$ is a unit in the power series ring $\mathcal{O}_{H,w}[[t_{\mathfrak{b},w}]]$.*

Proof. This is a well-known classical argument (see the proof of [**8**, Lemma 8]) and we omit the details. Note that we also use the fact that $c_{A^\mathfrak{b}}(\lambda)$ is a unit in $\mathcal{O}_{H,w}$ because it is shown in the Appendix to [**8**] that $c_\alpha(A^\mathfrak{b})^{12} = \Delta(A^\mathfrak{b})^{(N\alpha-1)}/\alpha^{12}$, where $\Delta(A^\mathfrak{b})$ is the discriminant of our global minimal equation for $A^\mathfrak{b}$, and we have $(\mathfrak{p}, \Delta(A^\mathfrak{b})\alpha) = 1$. □

We now turn to the fields $F_n = K(B_{\mathfrak{P}^{n+2}})$, where, of course, the only natural thing to do is to define the group of elliptic units $C(F_n)$ of F_n by

$$C(F_n) = N_{\mathfrak{F}_n/F_n}(C(\mathfrak{F}_n)), \tag{4.11}$$

where $N_{\mathfrak{F}_n/F_n}$ denotes the norm map from $\mathfrak{F}_n$ to F_n. Thus, writing

$$u_{\alpha,n} = N_{\mathfrak{F}_n/F_n}(\mathfrak{R}_{\alpha,A}(V_n)), \tag{4.12}$$

these $u_{\alpha,n}$ are global units in F_n, and, since the restriction of δ to $\mathfrak{F}_n$ lies in $\mathrm{Gal}(\mathfrak{F}_n/F_n)$, we conclude immediately from Theorem 4.6 that

$$N_{F_n/F_{n-1}}(u_{\alpha,n}) = u_{\alpha,n-1} \ \ (n \geqslant 1). \tag{4.13}$$

We write

$$u_{\alpha,\infty} = (u_{\alpha,n}) \tag{4.14}$$

for this norm compatible system of elliptic units. However, unlike the situation for the field $\mathfrak{F}_\infty$, it seems that these units $u_{\alpha,n}$ cannot be obtained for all $n \geqslant 0$ by evaluating a single rational function on A at the point V_n. All we can do in this direction is the following. Recall that $\mathfrak{C}_n$ denotes a set of integral ideals of K prime to $\mathfrak{pq}$ whose Artin symbols in $\mathrm{Gal}(\mathfrak{F}_n/K)$ give precisely $\mathrm{Gal}(\mathfrak{F}_n/F_n)$, and define the rational function $D_{\alpha,n}(P)$ on A/H by

$$D_{\alpha,n}(P) = \prod_{\mathfrak{c}\in\mathfrak{C}_n} \mathfrak{R}_{\alpha,A^\mathfrak{c}}(\eta_A(\mathfrak{c})(P)). \tag{4.15}$$

LEMMA 4.9. *For all integers n and k with $n \geqslant 0$ and $0 \leqslant k \leqslant n$, we have $D_{\alpha,n}(V_k) = u_{\alpha,k}$.*

Proof. This is clear from Lemma 4.3 and the fact that $\mathrm{Gal}(\mathfrak{F}_n/F_n)$ is isomorphic under restriction to $\mathrm{Gal}(\mathfrak{F}_k/F_k)$ for $0 \leqslant k \leqslant n$. □

LEMMA 4.10. *For each prime w of H above $\mathfrak{p}$, the rational function $D_{\alpha,n}(P)$ has a t_w-expansion $d_{\alpha,n}(t_w)$ which lies in $\mathcal{O}_{H,w}[[t_w]]$, and is a unit in this ring.*

Proof. By Lemma 4.8, for each $\mathfrak{c} \in \mathfrak{C}_n$, the rational function $\mathfrak{R}_{\alpha,A^{\mathfrak{c}}}(P_{\mathfrak{c}})$ has a $t_{\mathfrak{c},w}$-expansion which is a unit in $\mathcal{O}_{H,w}[[t_{\mathfrak{c},w}]]$. Now the isogeny $\eta_A(\mathfrak{c}) : A \to A^{\mathfrak{c}}$ induces a homomorphism of formal groups

$$\widehat{\eta_{A,\mathfrak{c},w}} : \widehat{A_w} \to \widehat{A^{\mathfrak{c}}_w},$$

where $\widehat{A_w}$ and $\widehat{A^{\mathfrak{c}}_w}$ denote the respective formal groups of A and $A^{\mathfrak{c}}$ at w. In particular, such a homomorphism is realized by a formal power series $t_{\mathfrak{c},w} = \widehat{\eta_{A,\mathfrak{c},w}}(t_w)$ in $\mathcal{O}_{H,w}[[t_w]]$ with $\widehat{\eta_{A,\mathfrak{c},w}}(0) = 0$. Substituting this formal power series in the unit power series expansion in $\mathcal{O}_{H,w}[[t_{\mathfrak{c},w}]]$ of $\mathfrak{R}_{\alpha,A^{\mathfrak{c}}}(P_{\mathfrak{c}})$, and taking the product over all $\mathfrak{c} \in \mathfrak{C}_n$, the assertion of the lemma follows. □

Now the power series ring $\mathcal{O}_{H,w}[[t_w]]$ is a regular local ring of dimension 2, which is complete for the topology defined by the powers of its maximal ideal $\mathfrak{m}$.

PROPOSITION 4.11. *For each prime w of H above $\mathfrak{p}$, the sequence of unit power series $d_{\alpha,m}(t_w)\,(m = 0, 1, \ldots)$ in $\mathcal{O}_{H,w}[[t_w]]$ converges to a unique unit power series $d_{\alpha,\infty}(t_w)$ in $\mathcal{O}_{H,w}[[t_w]]$, satisfying $d_{\alpha,\infty}(t_w(V_n)) = u_{\alpha,n}$ for all $n \geqslant 0$.*

Proof. For all $m_2 \geqslant m_1$, it follows from Lemma 4.9 that the power series

$$d_{\alpha,m_2}(t_w) - d_{\alpha,m_1}(t_w)$$

vanishes at the points $t_w(V_k)\,(k = 0, \ldots, m_1)$ and all conjugates of these points over H_w. Thus $d_{\alpha,m_2}(t_w) - d_{\alpha,m_1}(t_w)$ is divisible in $\mathcal{O}_{H,w}[[t_w]]$ by the monic polynomial $P_{m_1}(t_w)$ whose roots are given by all conjugates of the $t_w(V_k)(k = 0, \ldots, m_1)$ over H_w. Since it is easily seen that $P_{m_1}(t_w)$ tends to zero in the $\mathfrak{m}$-adic topology as $m_1 \to \infty$, it follows by completeness that the limit power series $d_{\alpha,\infty}(t_w) = \lim_{m\to\infty} d_{\alpha,m}(t_w)$ exists, and satisfies $d_{\alpha,\infty}(t_w(V_n)) = u_{\alpha,n}$ for all $n \geqslant 0$. This completes the proof. □

5. *Canonical measures attached to elliptic units*

The aim of this section is to show how to relate norm compatible systems of elliptic units in the tower F_∞/F to the complex L-values $L(\bar{\phi}^k, k)$ for all integers $k \geqslant 1$, again broadly following the method introduced in [**14**]. As always, δ always denotes the unique element of $\mathrm{Gal}(\mathfrak{F}_\infty/F_\infty)$ whose restriction to $\mathfrak{G}$ is the Artin symbol of $\mathfrak{p}$. Thus, for any place w of H above $\mathfrak{p}$, we can view δ as a generator of $\mathrm{Gal}(H_w/K_{\mathfrak{p}})$. If $J(P)$ is any rational function on A/H, we shall write $J^\delta(P_{\mathfrak{p}})$ for the rational function on $A^{\mathfrak{p}}/H$ obtained by applying δ to the coefficients of $J(P)$.

We first establish the following analogue of (4.10).

LEMMA 5.1. *For all $n \geqslant 0$, we have*

$$D^\delta_{\alpha,n}(\eta_A(\mathfrak{p})(P)) = \prod_{V \in A_{\mathfrak{p}}} D_{\alpha,n}(P \oplus V). \tag{5.1}$$

Proof. For each $\mathfrak{c} \in \mathfrak{C}_n$, we have the equality of isogenies

$$\eta_{A^{\mathfrak{p}}}(\mathfrak{c}) \circ \eta_A(\mathfrak{p}) = \eta_{A^{\mathfrak{c}}}(\mathfrak{p}) \circ \eta_A(\mathfrak{c}) = \eta_A(\mathfrak{cp}),$$

whence it follows easily that

$$D^{\delta}_{\alpha,n}(\eta_A(\mathfrak{p})(P)) = \prod_{\mathfrak{c}\in\mathfrak{C}_n} \mathfrak{R}_{\alpha,A^{\mathfrak{cp}}}(\eta_{A^{\mathfrak{c}}}(\mathfrak{p})(\eta_A(\mathfrak{c})(P))). \tag{5.2}$$

Since $\mathfrak{p}$ is prime to α, the good behavior of the R-functions with respect to isogeny (see [8, Theorem 4]) shows that

$$\mathfrak{R}_{\alpha,A^{\mathfrak{cp}}}(\eta_{A^{\mathfrak{c}}}(\mathfrak{p})(P_{\mathfrak{c}})) = \prod_{W\in A^{\mathfrak{c}}_{\mathfrak{p}}} \mathfrak{R}_{\alpha,A^{\mathfrak{c}}}(P_{\mathfrak{c}} \oplus W).$$

The assertion of the lemma then follows on noting that the isogeny $\eta_A(\mathfrak{c})$ maps $A_{\mathfrak{p}}$ isomorphically to $A^{\mathfrak{c}}_{\mathfrak{p}}$ because of our assumption that $(\mathfrak{c},\mathfrak{p}) = 1$ for $\mathfrak{c} \in \mathfrak{C}_n$. This completes the proof. □

As in the previous section, we write $d_{\alpha,n}(t_w)$ for the formal power series expansion of the rational function $D_{\alpha,n}(P)$ on A/H in terms of the parameter t_w of the formal group of A at w, say $d_{\alpha,n}(t_w) = \sum_{k\geqslant 0} e_{\alpha,n}(k)t_w^k$. It is then clear that the rational function $D^{\delta}_{\alpha,n}(P_{\mathfrak{p}})$ on $A^{\mathfrak{p}}$ has the expansion in terms of the parameter $t_{\mathfrak{p},w}$ of the formal group of $A^{\mathfrak{p}}$ at w given by $d^{\delta}_{\alpha,n}(t_{\mathfrak{p},w}) = \sum_{k\geqslant 0} \delta(e_{\alpha,n}(k))t^k_{\mathfrak{p},w}$. Moreover, since $d_{\alpha,\infty}(t_w) = \lim_{n\to\infty} d_{\alpha,n}(t_w)$, we see that $\lim_{n\to\infty} d^{\delta}_{\alpha,n}(t_{\mathfrak{p},w})$ also exists, and we denote this limit by $d^{\delta}_{\alpha,\infty}(t_{\mathfrak{p},w})$. All of these formal power series are, of course, units. Then the key first step for constructing our measures is to define, for $0 \leqslant n \leqslant \infty$, the power series

$$\mathfrak{D}_{\alpha,n,w}(t_w) = d_{\alpha,n}(t_w)^2 / d^{\delta}_{\alpha,n}(\widehat{\eta_{A,\mathfrak{p},w}}(t_w)), \tag{5.3}$$

where, as before, $\widehat{\eta_{A,\mathfrak{p},w}} : \widehat{A}_w \to \widehat{A}^{\mathfrak{p}}_w$ is the map between formal groups induced by the isogeny $\eta_A(\mathfrak{p})$.

LEMMA 5.2. *For $0 \leqslant n \leqslant \infty$, the power series $\mathfrak{D}_{\alpha,n,w}(t_w)$ lies in $1 + \mathfrak{m}_{H,w}[[t_w]]$, where $\mathfrak{m}_{H,w}$ denotes the maximal ideal of $\mathcal{O}_{H,w}$.*

Proof. Since ϕ is the Serre–Tate character of B/K, the reduction of the endomorphism $\phi(\mathfrak{p})$ of B must be the Frobenius endomorphism of the reduction of B modulo $\mathfrak{p}$, from which it follows easily that

$$\widehat{\eta_{A,\mathfrak{p},w}}(t_w) \equiv t_w^2 \bmod \mathfrak{m}_{H,w}. \tag{5.4}$$

Hence

$$d^{\delta}_{\alpha,n}(\widehat{\eta_{A,\mathfrak{p},w}}(t_w)) = \sum_{k=0}^{\infty} \delta(e_{\alpha,n}(k))(\widehat{\eta_{A,\mathfrak{p},w}}(t_w))^k \equiv \sum_{k=0}^{\infty} e_{\alpha,n}(k)^2 t_w^{2k} \bmod \mathfrak{m}_{H,w}.$$

On the other hand, $d_{\alpha,n}(t_w)^2$ has t_w-expansion

$$\left(\sum_{k=0}^{\infty} e_{\alpha,n}(k)t_w^k\right)^2 \equiv \sum_{k=0}^{\infty} e_{\alpha,n}(k)^2 t_w^{2k} \bmod \mathfrak{m}_{H,w},$$

whence the power series (5.3) does indeed lie in $1 + \mathfrak{m}_{H,w}[[t_w]]$, as claimed. □

LEMMA 5.3. *For $0 \leqslant n \leqslant \infty$, the power series $J_{\alpha,n,w}(t_w) = \frac{1}{2} log(\mathfrak{D}_{\alpha,n,w}(t_w))$ lies in $\mathcal{O}_{H,w}[[t_w]]$, and satisfies the identity*

$$\sum_{V \in A_{\mathfrak{p}}} J_{\alpha,n,w}(t_w[+]t_w(V)) = 0, \tag{5.5}$$

where $[+]$ denotes the group law of the formal group of $\widehat{A_w}$.

Proof. The first assertion follows immediately from Lemma 5.2 because H_w is an unramified extension of $\mathbb{Q}_2$. Moreover, for $0 \leqslant n \leqslant \infty$, Lemma 5.1 shows that

$$\prod_{V \in A_{\mathfrak{p}}} \mathfrak{D}_{\alpha,n}(t_w[+]t_w(V)) = 1. \tag{5.6}$$

But then we conclude that this identity must also hold for $n = \infty$ by passage to the limit as $n \to \infty$. The second assertion of the lemma now follows on taking logarithms, and noting that the points in $A_{\mathfrak{p}}$ do indeed lie on the formal group $\widehat{A_w}$. □

We now fix an embedding of H into the maximal unramified extension of $K_{\mathfrak{p}}$ which induces the prime w of H. We recall that $\mathscr{I}$ denotes the ring of integers of the completion of the maximal unramified extension of $K_{\mathfrak{p}}$. Since the formal group $\widehat{A_w}$ has height 1, a classical theorem asserts that it is isomorphic over $\mathscr{I}$ to the formal multiplicative group $\widehat{\mathbb{G}}_m$, and we fix such an isomorphism

$$j_w : \widehat{\mathbb{G}}_m \simeq \widehat{A_w}. \tag{5.7}$$

Writing W for the parameter of the formal multiplicative group, the isomorphism j_w can be viewed as being given by a formal power series $t_w = j_w(W)$ in W with coefficients in $\mathscr{I}$ of the form $j_w(W) = \Omega_w(A)W + \cdots$, where $\Omega_w(A)$ is a unit in $\mathscr{I}$. For $0 \leqslant n \leqslant \infty$, we can then define the power series

$$\mathfrak{J}_{\alpha,n,w}(W) = J_{\alpha,n,w}(j_w(W)), \tag{5.8}$$

which, in view of (5.5), satisfies

$$\sum_{\zeta \in \mu_2} \mathfrak{J}_{\alpha,n,w}(\zeta(1+W) - 1) = 0, \tag{5.9}$$

where $\mu_2 = \{\pm 1\}$. Recall that $\Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}})$ (respectively, $\Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}}^{\times})$) denotes the ring of $\mathscr{I}$-valued measures on $\mathcal{O}_{\mathfrak{p}}$ (respectively, $\mathcal{O}_{\mathfrak{p}}^{\times}$). Thanks to Mahler's beautiful theorem on the characterization of continuous 2-adic valued functions on $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_2$, we have the topological ring isomorphism

$$\mathbb{M} : \Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}}) \simeq \mathscr{I}[[W]], \tag{5.10}$$

which is defined by $\mathbb{M}(\mu) = \sum_{n \geqslant 0} a_n(\mu) W^n$, where $a_n(\mu) = \int_{\mathcal{O}_{\mathfrak{p}}} \binom{x}{n} d\mu$ for all $n \geqslant 0$. Now we have the inclusion $i : \Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}}^{\times}) \to \Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}})$ given by extending a measure on $\mathcal{O}_{\mathfrak{p}}^{\times}$ to $\mathcal{O}_{\mathfrak{p}}$ by zero. Moreover, it is well known that a measure μ belongs to $i(\Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}}^{\times}))$ if and only if $\mathbb{M}(\mu)$ satisfies the equation

$$\sum_{\zeta \in \mu_2} \mathbb{M}(\mu)(\zeta(1+W) - 1) = 0. \tag{5.11}$$

In particular, we conclude from (5.9) that, for all n with $0 \leqslant n \leqslant \infty$ there exists a unique measure $\mu_{\alpha,n,w}$ in $\Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}}^{\times})$ such that $\mathbb{M}(i(\mu_{\alpha,n,w})) = \mathfrak{J}_{\alpha,n,w}(W)$. Recalling that we can

canonically identify the Galois group G with $\mathcal{O}_{\mathfrak{p}}^{\times}$ via the character $\rho_{\mathfrak{P}}$, we shall in what follows always view the $\mu_{\alpha,n,w}$ as $\mathscr{I}$-valued measures on G. Moreover, we have

$$\mu_{\alpha,\infty,w} = \lim_{n\to\infty} \mu_{\alpha,n,w}. \tag{5.12}$$

In the following, when there is no danger of confusion about the place w of H lying above $\mathfrak{p}$, we shall simply write $\mu_{\alpha,\infty}$ for $\mu_{\alpha,\infty,w}$.

We recall that we have fixed an embedding of the field $\mathscr{T}$ into $\mathbb{C}$ which extends our embedding of K into $\mathbb{C}$, so that we can then consider the complex Hecke L-functions $L(\bar{\phi}^k, s)$ for all integers $k \geqslant 1$. Now the Hecke character $\bar{\phi}^k$ has conductor $\mathfrak{q}$ or $\mathcal{O}_K$, according to k is odd or even. For all $k \geqslant 1$, we shall write $L_{\mathfrak{q}}(\bar{\phi}^k, s)$ for the Euler product with the Euler factor at $\mathfrak{q}$ removed (so that this L-series is imprimitive when k is even). Finally, we fix an embedding of the compositum $\mathscr{T}H$ into the fraction field of $\mathscr{I}$ which induces the prime w of H and the prime $\mathfrak{P}$ of $\mathscr{T}$. This is possible because $H \cap \mathscr{T} = K$.

THEOREM 5.4. *For all integers $k \geqslant 1$, the values $\Omega_\infty(A)^{-k} L_{\mathfrak{q}}(\bar{\phi}^k, k)$ belong to $\mathscr{T}H$, and we have*

$$\Omega_{\mathfrak{p}}(A)^{-k} \int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,\infty} = b_k(\alpha)(k-1)!\Omega_\infty(A)^{-k} L_{\mathfrak{q}}(\bar{\phi}^k, k)(1 - \phi^k(\mathfrak{p})/N\mathfrak{p}), \tag{5.13}$$

where $b_k(\alpha) = (-1)^{k-1}(\sqrt{-q})^k(\phi^k((\alpha)) - N\alpha)$.

The crucial step in proving this theorem is the following classical result. If $\mathfrak{b}$ is any integral ideal of K prime to $\mathfrak{q}$, we write $\gamma_{\mathfrak{b}}$ for the class of $\mathfrak{b}$. We then define the partial Hecke L-function $L_{\mathfrak{q}}(\bar{\phi}^k, \gamma_{\mathfrak{b}}, s)$ by

$$L_{\mathfrak{q}}(\bar{\phi}^k, \gamma_{\mathfrak{b}}, s) = \sum_{\mathfrak{c} \in \gamma_{\mathfrak{b}}} \frac{\bar{\phi}^k(\mathfrak{c})}{(N\mathfrak{c})^s}, \tag{5.14}$$

where the sum is taken over all integral ideals $\mathfrak{c}$ of K, which are prime to $\mathfrak{q}$, and which lie in the class $\gamma_{\mathfrak{b}}$.

PROPOSITION 5.5. *Let $\mathfrak{b}$ be any integral ideal of K prime to $\mathfrak{q}$. Then, for all $\alpha \in \mathscr{J}$, we have*

$$\frac{d}{dz} \log(\mathfrak{R}_{\alpha,A^{\mathfrak{b}}}(\eta_A(\mathfrak{b})(\mathcal{W}(z,\mathcal{L})))) = \sum_{k=1}^{\infty} b_k(\alpha)\phi(\mathfrak{b})^k \Omega_\infty(A)^{-k} L_{\mathfrak{q}}(\bar{\phi}^k, \gamma_{\mathfrak{b}}, k) z^{k-1}. \tag{5.15}$$

where $b_k(\alpha) = (-1)^{k-1}(\sqrt{-q})^k(\phi((\alpha))^k - N\alpha)$.

Proof. The proof rests upon a miraculous product formula from the nineteenth century theory of elliptic functions. We recall rapidly this product formula, and its link with our rational functions $\mathfrak{R}_{\alpha,A^{\mathfrak{b}}}$, without giving a fully detailed, but essentially straightforward, proof of the Proposition. Let L be any lattice in $\mathbb{C}$, say $L = u\mathbb{Z} + v\mathbb{Z}$, with v/u having positive imaginary part. We define

$$A(L) = (\overline{u}v - \overline{v}u)/2\pi i, \;\; s_2(L) = \lim_{s\to 0} \sum_{\omega \neq 0 \in L} \omega^{-2}|\omega|^{-2s},$$

where the limit is taken over real values of $s > 0$. For each integer $k \geqslant 1$, we have the Kronecker–Eisenstein series

$$H_k(z, s, L) = \sum_{\omega \in L} \frac{(\overline{z} + \overline{\omega})^k}{|z + \omega|^{2s}},$$

where we assume that $z \notin L$. This series converges in the half plane $R(s) > 1 + k/2$, but it has a holomorphic continuation to the whole s-plane. We then define

$$\mathcal{E}_k^*(z, L) = H_k(z, k, L).$$

The all important classical infinite product which we use is

$$\sigma(z, L) = z \prod_{\omega \in L \setminus 0} (1 - z/\omega) \exp(z/\omega + \tfrac{1}{2}(z/\omega)^2),$$

and we then define

$$\theta(z, L) = \exp(-s_2(L) z^2/2)\sigma(z, L).$$

Taking logarithmic derivatives, we easily obtain from the infinite product that, for all $z_0 \in \mathbb{C}$ with $z_0 \notin L$, we have

$$\frac{d}{dz} \log(\theta(z + z_0, L)) = \overline{z_0}/A(L) + \sum_{k=1}^{\infty} (-1)^{(k-1)} \mathcal{E}_k^*(z_0, L) z^{k-1}. \tag{5.16}$$

We now take these functions for the lattice $\mathcal{L}_{\mathfrak{b}}$, and we have the following equality (see [**19**, Theorem 1.9]):

$$R_{\alpha, A^{\mathfrak{b}}}(\mathcal{W}(z, \mathcal{L}_{\mathfrak{b}}))^2 = c_\alpha(A_{\mathfrak{b}})^2 \theta(z, \mathcal{L}_{\mathfrak{b}})^{2N\alpha} / \theta(z, \alpha^{-1}\mathcal{L}_{\mathfrak{b}})^2. \tag{5.17}$$

Now take $\mathfrak{E}$ to be any set of integral of K, prime to $\mathfrak{q}$, whose Artin symbols in $\mathrm{Gal}(H(A_{\mathfrak{q}})/K)$ give precisely $\mathrm{Gal}(H(A_{\mathfrak{q}})/H)$. Recalling that $H(A_{\mathfrak{q}}) = H(A_{\mathfrak{q}}^{\mathfrak{b}})$, and taking the $\mathfrak{q}$-division point on $A^{\mathfrak{b}}$ given by $Q(\mathfrak{b}) = \mathcal{W}(\xi(\mathfrak{b})\Omega_\infty(A)/\sqrt{-q}, \mathcal{L}_{\mathfrak{e}})$, we then have (see [**19**, Proposition 5.5])

$$(\sqrt{-q})^k (\phi(\mathfrak{b})/\xi(\mathfrak{b}))^k \Omega_\infty(A)^{-k} L(\overline{\phi}^k, \gamma_{\mathfrak{b}}, k) = \sum_{\mathfrak{e} \in \mathfrak{E}} \mathcal{E}_k^*(\phi(\mathfrak{e})\xi(\mathfrak{b})\Omega_\infty(A)/\sqrt{-q}, \mathcal{L}_{\mathfrak{b}}). \tag{5.18}$$

On combining equations (5.16), (5.17), (5.18), recalling the definition (4.8), and noting that

$$\eta_A(\mathfrak{b})(\mathcal{W}(z, \mathcal{L})) = \mathcal{W}(\xi(\mathfrak{b})z, \mathcal{L}_{\mathfrak{b}}), \tag{5.19}$$

the formula (5.15) follows easily. This completes the proof. □

Corollary 5.6. *For all integral ideals $\mathfrak{b}$ of K prime to $\mathfrak{q}$ and all integers $k \geqslant 1$,*

$$b_k(\alpha)\phi(\mathfrak{b})^k (k-1)! \Omega_\infty(A)^{-k} L_{\mathfrak{q}}(\overline{\phi}^k, \gamma_{\mathfrak{b}}, k)$$

belongs to H and is integral at w.

Proof. Since $\mathfrak{R}_{\alpha, A^{\mathfrak{b}}}(\eta_A(\mathfrak{b})(P))$ is a rational function on A/H, the first assertion is clear from (5.15). Moreover, we have already seen (see Lemma 4.8) that this rational function has an expansion, in terms of the parameter t_w of the formal group $\widehat{A_w}$, which is a unit in $\mathcal{O}_{H,w}[[t_w]]$. Now we can interpret the differential operator d/dz in terms of the formal group $\widehat{A_w}$ as follows. The exponential map of $\widehat{A_w}$ is given by expanding $t_w = \nu_w(z)$, where $\nu_w(z)$ is given by expanding the right-hand side of

$$t_w = -2(\wp(z, \mathcal{L}) - b_2/12)/(\wp'(z, \mathcal{L}) - a_1(\wp(z, \mathcal{L}) - b_2/12) - a_3), \tag{5.20}$$

as a power series in z. The logarithm map of $\widehat{A_w}$ is given by the inverse series under composition, say

$$z = \lambda_w(t_w). \tag{5.21}$$

We shall simply write $\lambda_w'(t_w)$ for the formal derivative of the power series $\lambda_w(t_w)$ with respect to t_w. By one of the basic properties of such a logarithm map, $\lambda_w'(t_w)$ is in fact a unit

power series in $\mathcal{O}_{H,w}[[t_w]]$. But we have $d/dz = (\lambda'(t_w))^{-1}d/dt_w$. Hence, since the t_w-expansion of $\mathfrak{R}_{\alpha,A^{\mathfrak{b}}}(\eta_A(\mathfrak{b})(P))$ is a unit in $\mathcal{O}_{H,w}[[t_w]]$, we conclude that, for all integers $k \geqslant 1$, the t_w-expansion of $(d/dz)^k \log \mathfrak{R}_{\alpha,A^{\mathfrak{b}}}(\eta_A(\mathfrak{b})(P))$ will lie in $\mathcal{O}_{H,w}[[t_w]]$. In particular, its constant term will lie in $\mathcal{O}_{H,w}$, proving the second assertion of the corollary. □

PROPOSITION 5.7. *For all integers $n \geqslant 0$ and $k \geqslant 1$, we have*

$$\Omega_{\mathfrak{p}}(A)^{-k} \int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,n} = b_k(\alpha)(k-1)!\Omega_\infty(A)^{-k} \sum_{\mathfrak{c}\in\mathfrak{C}_n} \phi^k(\mathfrak{c})(L_{\mathfrak{q}}(\bar{\phi}^k, \gamma_{\mathfrak{c}}, k) - \frac{\phi(\mathfrak{p})^k}{N\mathfrak{p}} L_{\mathfrak{q}}(\bar{\phi}^k, \gamma_{\mathfrak{c}\mathfrak{p}}, k)). \tag{5.22}$$

Proof. The exponential map of the formal group $\widehat{\mathbb{G}_m}$ is given by $W = e^z - 1$. Thus, by the uniqueness of the exponential map for $\widehat{A_w}$, it follows that we must have

$$t_w = \nu_w(z) = j_w(e^{z/\Omega_v(A)} - 1). \tag{5.23}$$

Now it is very well known (see, for example, [**12**]) that, for all integers $k \geqslant 1$, we have

$$\int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,n} = \int_{\mathbb{Z}_2} x^k d\mu_{\alpha,n} = (d/dz)^k \mathfrak{J}_{\alpha,n}(W)|_{z=0}. \tag{5.24}$$

But obviously

$$(d/dz)^k \mathfrak{J}_{\alpha,n}(e^z - 1) = \Omega_v(A)^k (d/dz)^k \mathfrak{J}_{\alpha,n}(e^{z/\Omega_v(A)} - 1).$$

In view of (5.23), we conclude from (5.8) that

$$\Omega_v(A)^{-k} \int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,n} = (d/dz)^k \mathfrak{M}_{\alpha,n}(t_w)|_{z=0}. \tag{5.25}$$

But

$$\mathfrak{M}_{\alpha,n}(t_w) = \frac{1}{2} \sum_{\mathfrak{c}\in\mathfrak{C}_n} \log(\mathfrak{R}_{\alpha,A^{\mathfrak{c}}}(\eta_A(\mathfrak{c})(\mathcal{W}(z,\mathcal{L}))^2 / \mathfrak{R}_{\alpha,A^{\mathfrak{c}\mathfrak{p}}}(\eta_A(\mathfrak{c}\mathfrak{p})(\mathcal{W}(z,\mathcal{L}))).$$

Hence the conclusion of the proposition follows immediately from (5.25) and applying Proposition 5.5 with $\mathfrak{b} = \mathfrak{c}$ and $\mathfrak{b} = \mathfrak{c}\mathfrak{p}$. This completes the proof. □

We can now prove Theorem 5.4. In view of (5.12), we have, for all integers $k \geqslant 1$,

$$\int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,\infty} = \lim_{n\to\infty} \int_G \rho_{\mathfrak{P}}^k d\mu_{\alpha,n}.$$

We recall that we have fixed an embedding of the compositum $H\mathcal{T}$ into the fraction field of $\mathcal{I}$ which induces the prime w on H and the prime $\mathfrak{P}$ on $\mathcal{T}$. Recall also that for $\mathfrak{c} \in \mathfrak{C}_n$, we have $\phi(\mathfrak{c}) \equiv 1 \bmod \mathfrak{P}^{n+2}$. Moreover, for each $n \geqslant 0$, $\mathfrak{C}_n$ gives a complete set of representatives of the ideal class group of K. It is therefore clear that Theorem 5.4 will follow from on passing to the limit as $n \to \infty$ from (5.22). This completes the proof.

6. *Iwasawa theory of the local tower $K_{\mathfrak{p}}(B_{\mathfrak{P}^\infty})/K_{\mathfrak{p}}$*

We need to establish the local theory at the prime $\mathfrak{p}$ for the tower F_∞/K in order to prove the main conjecture. The local extension $K_{\mathfrak{p}}(B_{\mathfrak{P}^\infty})/K_{\mathfrak{p}}$ does not arise naturally from the points of finite order on a Lubin–Tate group. However, we take a prime w of H above $\mathfrak{p}$, and we show that, since the class number of K is odd, we can fairly easily derive what is needed from the classical theory for the Lubin–Tate extension $H_w(A_{\mathfrak{p}^\infty})/H_w$.

Put $r = [H_w : K_\mathfrak{p}]$, so that r is the order of both δ, and the ideal class of $\mathfrak{p}$, and, of course, r is odd because it divides the class number of K. Define

$$H_{w,\infty} = H_w(A_{\mathfrak{p}^\infty}),\ F_{\infty,\mathfrak{p}} = K_\mathfrak{p}(B_{\mathfrak{P}^\infty}), \tag{6.1}$$

and put

$$\mathcal{G}_w = \mathrm{Gal}(H_{w,\infty}/H_w),\ \mathfrak{G}_{w,\infty} = \mathrm{Gal}(H_{w,\infty}/K_\mathfrak{p}),\ \Delta_w = \mathrm{Gal}(H_{w,\infty}/F_{\infty,\mathfrak{p}}), \tag{6.2}$$

so that $\mathfrak{G}_{w,\infty} = \mathcal{G}_w \times \Delta_w$. Of course, $H_w/K_\mathfrak{p}$ is unramified, $\mathfrak{p}$ is totally ramified in $F_{\infty,\mathfrak{p}}$, and w is totally ramified in $H_{w,\infty}$. Let $F_{n,\mathfrak{p}} = K_\mathfrak{p}(B_{\mathfrak{P}^{n+2}})$ and $H_{n,w} = H_w(A_{\mathfrak{p}^{n+2}})$, and write $U(F_{n,\mathfrak{p}})$ and $U(H_{n,w})$ for their respective groups of local units. Define

$$U(F_{\infty,\mathfrak{p}}) = \varprojlim_n U(F_{n,\mathfrak{p}}),\ U(H_{\infty,w}) = \varprojlim_n U(H_{n,w}), \tag{6.3}$$

where the projective limits are taken with respect to the local norm maps. We recall that we have fixed a set $\{V_n\}$ of primitive $\mathfrak{p}^{n+2}$-division points on A, which are compatible in the sense that (2.13) holds for all $n \geqslant 0$. We write, as before, t_w for the parameter of the formal group $\widehat{A_w}$ of A at w, and $\mathcal{O}_{H,w}$ for the ring of integers of H_w. The following is de Shalit's extension of Coleman's theorem [18].

THEOREM 6.1. *For each $\mathfrak{u}_\infty = (\mathfrak{u}_n)$ in $U(H_{\infty,w})$, there exists a unique power series $C_{\mathfrak{u}_\infty}(t_w)$ in $\mathcal{O}_{H,w}[[t_w]]$ such that $\mathfrak{u}_n = \delta^{-n}(C_{\mathfrak{u}_\infty}(t_w(V_n)))$ for all $n \geqslant 0$.*

We shall also need the following corollary of this theorem.

COROLLARY 6.2. *For each $u_\infty = (u_n)$ in $U(F_{\infty,\mathfrak{p}})$, there exists a unique power series $C_{u_\infty}(t_w)$ in $\mathcal{O}_{H,w}[[t_w]]$ such that $u_n = C_{u_\infty}(t_w(V_n))$ for all $n \geqslant 0$.*

To deduce the corollary from the theorem, we note that, for all $m \geqslant n$, $\mathrm{Gal}(\mathfrak{F}_{m,w}/\mathfrak{F}_{n,w})$ is isomorphic to $\mathrm{Gal}(F_{m,\mathfrak{p}}/F_{n,\mathfrak{p}})$ under restriction. Hence u_∞ clearly can be viewed as an element of $U(H_{\infty,w})$, and so has its Coleman power series $C_{u_\infty}(t_w)$. This Coleman power series then has the interpolation property stated in the corollary because $\delta^n(u_n) = u_n$ for all $n \geqslant 0$. The uniqueness in both results is obvious from the Weierstrass Preparation Theorem.

Let $\mathfrak{u}_\infty = (\mathfrak{u}_n)$ be any element of $U(H_{\infty,w})$, with Coleman power series $C_{\mathfrak{u}_\infty}(t_w)$. Define

$$\mathfrak{C}_{\mathfrak{u}_\infty}(t_w) = C_{\mathfrak{u}_\infty}(t_w)^2/C^\delta_{\mathfrak{u}_\infty}(\widehat{\eta_{A,\mathfrak{p},w}}(t_w)). \tag{6.4}$$

LEMMA 6.3. *The power series $\mathfrak{A}_{\mathfrak{u}_\infty}(t_w) = \frac{1}{2}\log \mathfrak{C}_{\mathfrak{u}_\infty}(t_w)$ lies in $\mathcal{O}_{H,w}[[t_w]]$, and satisfies the identity*

$$\sum_{V \in A_\mathfrak{p}} \mathfrak{A}_{\mathfrak{u}_\infty}(t_w[+]t_w(V)) = 0, \tag{6.5}$$

where $[+]$ denotes the group law of the formal group of $\widehat{A_w}$.

Proof. An entirely similar argument to that given in the proof of Lemma 5.2 shows that $\mathfrak{C}_{\mathfrak{u}_\infty}(t_w)$ belongs to $1 + \mathfrak{m}_{H,w}[[t_w]]$, and so the first assertion of the lemma follows. Moreover, it is shown in [18] (see Proposition 2.1 on p. 12 and Corollary 2.3, (ii) on p. 14) that

$$C^\delta_{\mathfrak{u}_\infty}(\widehat{\eta_{A,\mathfrak{p},w}}(t_w)) = \prod_{V \in A_\mathfrak{p}} C_{\mathfrak{u}_\infty}(t_w[+]t_w(V)),$$

whence the second assertion of the lemma also follows easily on taking logarithms. □

Recall (5.7) that we have fixed an $\mathscr{I}$-isomorphism $j_w : \widehat{\mathbb{G}}_m \simeq \widehat{A_w}$, and so, writing W for the parameter of the formal multiplicative group, we can then define the power series

$$\mathfrak{B}_{\mathfrak{u}_\infty}(W) = \mathfrak{A}_{\mathfrak{u}_\infty}(j_w(W)). \tag{6.6}$$

In view of (6.5), it follows, on applying Mahler's theorem to the power series $\mathfrak{B}_{\mathfrak{u}_\infty}(W)$, that there exists an $\mathscr{I}$-valued measure $\mu(\mathfrak{u}_\infty)$ on $\mathcal{O}_\mathfrak{p}^\times$ such that $\mathbb{M}(i(\mu(\mathfrak{u}_\infty))) = \mathfrak{B}_{\mathfrak{u}_\infty}(W)$. However, we now view $\mu(\mathfrak{u}_\infty)$ as a measure on the Galois group $\mathcal{G}_w$ via the canonical isomorphism $\rho_\mathfrak{p} : \mathcal{G}_w \to \mathcal{O}_\mathfrak{p}^\times$. Recall that $\mathfrak{G}_{w,\infty} = \mathcal{G}_w \times \Delta_w$. Following [18], we then define the measure $\tilde{\mu}(\mathfrak{u}_\infty)$ in $\Lambda_\mathscr{I}(\mathfrak{G}_{w,\infty})$ by

$$\tilde{\mu}(\mathfrak{u}_\infty) = \sum_{\sigma \in \Delta_w} \sigma\mu(\sigma^{-1}(\mathfrak{u}_\infty)). \tag{6.7}$$

This enables us to define the $\mathscr{I}$-linear $\mathfrak{G}_{w,\infty}$-homomorphism

$$j_{H_{w,\infty}} : U(H_{w,\infty})\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to \Lambda_\mathscr{I}(\mathfrak{G}_{w,\infty}) \tag{6.8}$$

by $j_{H_{w,\infty}}(\mathfrak{u}_\infty \otimes 1) = \tilde{\mu}(\mathfrak{u}_\infty)$. De Shalit (see [18, Chapter 1, Theorem 3.6]) then goes on to prove that $j_{H_{w,\infty}}$ is injective, and has a cokernel of the form $\mathfrak{W}_w \otimes_{\mathcal{O}_\mathfrak{p}} \mathscr{I}$, where $\mathfrak{W}_w$ is a finite $\mathfrak{G}_{w,\infty}$-module. On the other hand, if we take any $u_\infty \in U(F_{\infty,\mathfrak{p}})$, and define the power series $\mathfrak{B}_{u_\infty}(W)$ attached to u_∞ by exactly the same procedure as above, we again obtain by Mahler's theorem a measure $\mu(u_\infty)$ on $\mathcal{O}_\mathfrak{p}^\times$. However, in this case, we view $\mu(u_\infty)$ as a measure on the Galois group G via the canonical isomorphism $\rho_\mathfrak{P} : G \to \mathcal{O}_\mathfrak{p}^\times$. This in turn enables us to define the canonical $\mathscr{I}$-linear G-homomorphism

$$j_{F_\infty} : U(F_{\infty,\mathfrak{p}})\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to \Lambda_\mathscr{I}(G) \tag{6.9}$$

by $j_{F_\infty}(u_\infty \otimes 1) = \mu(u_\infty)$.

PROPOSITION 6.4. *The map j_{F_∞} is an injective $\Lambda_\mathscr{I}(G)$-homomorphism, and its cokernel is of the form $\mathfrak{W} \otimes_{\mathcal{O}_\mathfrak{p}} \mathscr{I}$, where $\mathfrak{W}$ is a finite G-module.*

Proof. We first prove that j_{F_∞} is injective. If $\mu(u_\infty) = 0$, then we must $\mathfrak{C}_{u_\infty}(t_w) = 1$, and so

$$C_{u_\infty}(t_w)^2 = C_{u_\infty}^\delta(\widehat{\eta_{A,\mathfrak{p},w}}(t_w)). \tag{6.10}$$

Putting $t_w = t_w(V_n)$ in this equation, and recalling the compatibility relation (2.13), we conclude that $u_n^2 = u_{n-1}$ for all $n \geqslant 1$. Putting $t_w = t_w(V_0)$ in the equation, we also conclude that $u_0^2 = C_{u_\infty}(0)^\delta$. Finally, putting $t_w = 0$ in (6.8), we obtain $C_{u_\infty}(0)^2 = C_{u_\infty}(0)^\delta$, and so $C_{u_\infty}(0)^{2^r-1} = 1$, where r is the order of $\mathfrak{p}$ in the ideal class group of K. Thus $C_{u_\infty}(0) = 1$ because $F_\mathfrak{p}$ has residue class field $\mathbb{F}_2$. But the group μ_{2^∞} of all 2-power roots of unity, cannot belong to the completion of F_∞ at the unique prime above $\mathfrak{p}$. Indeed, if it did, then the field $H_w(A_{\mathfrak{p}^\infty})$ would have to also contain $A_{\mathfrak{p}^*\infty}$ by the Weil pairing, and this is impossible because this latter group of points would map injectively under reduction modulo w, which cannot be the case because the field $H_w(A_{\mathfrak{p}^\infty})$ has a finite residue field. Thus we must have $u_n = 1$ for all $n \geqslant 0$, and the proof of injectivity is complete.

We next show how the remaining assertion of the theorem can be derived from [18, Chapter 1, Theorem 3.6]. The local norm map $N_{H_{\infty,w}/F_{\infty,\mathfrak{p}}}$ extends by $\mathscr{I}$-linearity to a map $\theta_\infty : U(H_{\infty,w})\widehat{\otimes}\mathscr{I} \to U(F_{\infty,\mathfrak{p}})\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I}$. We note that θ_∞ is surjective, because if $u_\infty = (u_n)$ is any element of $U(F_\infty)$, then, noting that raising to the rth power is an automorphism of $U(F_{\infty,\mathfrak{p}})$ because r is odd, we can simply define the element $\mathfrak{u}_\infty = (u_n^{1/r})$ of $U(H_{\infty,w})$, whence clearly $N_{H_{\infty,w}/F_{\infty,\mathfrak{p}}}(\mathfrak{u}_\infty) = u_\infty$. Noting that every element ζ of $\Lambda_\mathscr{I}(\mathfrak{G}_{w,\infty})$ can be

written uniquely in the form $\zeta = \sum_{\sigma \in \Delta_w} \sigma^{-1} A(\sigma)$ with $A(\sigma)$ in $\Lambda_{\mathscr{I}}(\mathcal{G}_w)$, we can define the map $\lambda_\infty : \Lambda_{\mathscr{I}}(\mathfrak{G}_{w,\infty}) \to \Lambda_{\mathscr{I}}(G)$ by

$$\lambda_\infty(\zeta) = \sum_{\sigma \in \Delta_w} \widetilde{A(\sigma)}, \tag{6.11}$$

where $\widetilde{A(\sigma)}$ is the image of $A(\sigma)$ under the isomorphism from $\Lambda_{\mathscr{I}}(\mathcal{G}_w)$ to $\Lambda_{\mathscr{I}}(G)$ given by the restriction map. We then have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U(H_{\infty,w})\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} & \xrightarrow{j_{H_{w,\infty}}} & \Lambda_{\mathscr{I}}(\mathfrak{G}_{w,\infty}) & \longrightarrow & \mathfrak{W}_w \otimes_{\mathcal{O}_\mathfrak{p}} \mathscr{I} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta_\infty} & & \downarrow{\scriptstyle \lambda_\infty} & & \downarrow{\scriptstyle i_\infty} & & \\ 0 & \longrightarrow & U(F_{\infty,\mathfrak{p}})\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} & \xrightarrow{j_{F_\infty}} & \Lambda_{\mathscr{I}}(G) & \longrightarrow & Coker(j_{F_\infty}) & \longrightarrow & 0 \end{array} \tag{6.12}$$

The commutativity of the left-hand square is easily verified from the explicit description we have given of the maps θ_∞ and λ_∞. Since the middle vertical map is clearly surjective because r is odd, it follows that the right-hand vertical map is also surjective. Thus the above diagram shows that Theorem 6.4 does indeed follow from [**18**, Chapter 1, Theorem 3.6]. □

7. *Proof of the main conjecture*

We establish in this section the analogue for B/F_∞ of Iwasawa's [**23**] celebrated theorem on cyclotomic fields, which led to the discovery of the main conjectures in general. Recall that $G = \Gamma \times \Delta$, where

$$\Gamma = \mathrm{Gal}(F_\infty/F),\ \Delta = \mathrm{Gal}(F_\infty/K_\infty) = \{1, j\}. \tag{7.1}$$

For each $n \geqslant 0$, let $\bar{C}(F_n)$ denote the closure of $C(F_n)$ in $U(F_{n,\mathfrak{p}})$ in the $\mathfrak{p}$-adic topology, and define $\bar{C}(F_\infty) = \varprojlim_n \bar{C}(F_n)$, where the projective limit is taken with respect to the local norm maps. Recalling that $U(F_{\infty,\mathfrak{p}}) = \varprojlim_n U(F_{n,\mathfrak{p}})$, we then define the G-module

$$Z(F_\infty) = U(F_{\infty,\mathfrak{p}})/\bar{C}(F_\infty). \tag{7.2}$$

We also define

$$U'(F_\mathfrak{p}) = \cap_{n \geqslant 0} N_n(U(F_{n,\mathfrak{p}})). \tag{7.3}$$

where N_n denotes the local norm map from $F_{n,\mathfrak{p}}$ to $F_\mathfrak{p}$. Thanks to (4.13), we see that we have $\bar{C}(F) \subset U'(F_\mathfrak{p})$.

PROPOSITION 7.1. *We have* $(Z(F_\infty))_\Gamma = U'(F_\mathfrak{p})/\bar{C}(F)$.

We first establish several preliminary results needed for the proof of this Proposition. Write $N_{F/K}$ for the global norm map from F to K, or the local norm map from $F_\mathfrak{p}$ to $K_\mathfrak{p}$.

LEMMA 7.2. *An element u of $U(F_\mathfrak{p})$ lies in $U'(F_\mathfrak{p})$ if and only if $N_{F/K}(u) = 1$.*

Proof. We first note that an element z of $U(K_\mathfrak{p})$ is a norm from $F_{n,\mathfrak{p}}$ for all $n \geqslant 0$ if and only if $z = 1$. Indeed, since $\mathfrak{p}$ is totally ramified in F_n and $\mathrm{Gal}(F_{n,\mathfrak{p}}/K_\mathfrak{p}) = (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{n+2})^\times$, it follows easily from local class field theory that $N_{F_n/K_\mathfrak{p}}(U(F_{n,\mathfrak{p}})) = 1 + \mathfrak{p}^{n+2}\mathcal{O}_\mathfrak{p}$, whence the previous assertion is clear. Now assume that u is any element of $U(F_\mathfrak{p})$. If u lies in $U'(F_\mathfrak{p})$, then $z = N_{F/K}(u)$ is an element of $U(K_\mathfrak{p})$ which is a norm from $U(F_{n,\mathfrak{p}})$ for all $n \geqslant 0$, and so z must be 1 by our first remark. Conversely, suppose u is any element of $U(F_\mathfrak{p})$ with $N_{F/K}(u) = 1$. Now the restriction map from $\mathrm{Gal}(F_{n,\mathfrak{p}}/F_\mathfrak{p})$ to $\mathrm{Gal}(K_{n,\mathfrak{p}}/K_\mathfrak{p})$ is an isomorphism for all $n \geqslant 0$.

Moreover, the local Artin symbol of u for the extension $F_{n,\mathfrak{p}}/F_{\mathfrak{p}}$, say σ restricts to the local Artin symbol of $N_{F/K}(u)$ for the extension $K_{n,\mathfrak{p}}/K_{\mathfrak{p}}$, which is equal to the identity. Hence $\sigma = 1$, and so by local class field theory, u must be a norm from $U(F_{n,\mathfrak{p}})$, and the proof is complete. □

LEMMA 7.3. *The natural projection of $U(F_{\infty,\mathfrak{p}})$ onto $U'(F_{\mathfrak{p}})$ induces an isomorphism $(U(F_{\infty,\mathfrak{p}}))_\Gamma = U'(F_{\mathfrak{p}})$.*

Proof. This is essentially an exercise in classical Iwasawa theory, whose proof we briefly sketch. Let $Y(F_{\infty,\mathfrak{p}})$ be the Galois group over $F_{\infty,\mathfrak{p}}$ of the maximal abelian 2-extension of $F_{\infty,\mathfrak{p}}$, and let $Y(F_{\mathfrak{p}})$ be the Galois group over $F_{\infty,\mathfrak{p}}$ of the maximal abelian 2-extension of $F_{\mathfrak{p}}$. As usual, $\Gamma = \mathrm{Gal}(F_{\infty,\mathfrak{p}}/F_{\mathfrak{p}})$ acts on $Y(F_{\infty,\mathfrak{p}})$, and we have

$$(Y(F_{\infty,\mathfrak{p}}))_\Gamma = Y(F_{\mathfrak{p}}). \tag{7.4}$$

On the other hand, Lubin–Tate theory shows that

$$Y(F_{\infty,\mathfrak{p}}) = U(F_{\infty,\mathfrak{p}}) \times \mathbb{Z}_2, \tag{7.5}$$

where $\mathbb{Z}_2$ denotes the Galois group of the maximal unramified 2-extension of $F_{\infty,\mathfrak{p}}$. Since clearly $U(F_{\infty,\mathfrak{p}})^\Gamma = 0$, we conclude that $Y(F_{\infty,\mathfrak{p}})^\Gamma$ is equal to the Galois group of the maximal unramified 2-extension of $F_{\infty,\mathfrak{p}}$. Viewing (7.5) as a short exact sequence for the Γ-module $Y(F_{\infty,\mathfrak{p}})$ with $U(F_{\infty,\mathfrak{p}})$ as submodule and $\mathbb{Z}_2$ as quotient, and taking Γ-cohomology of this exact sequence, we obtain from the snake lemma the exact sequence

$$0 \to U(F_{\infty,\mathfrak{p}})_\Gamma \to Y(F_{\infty,\mathfrak{p}})_\Gamma \to \mathbb{Z}_2 \to 0. \tag{7.6}$$

On the other hand, we have the short exact sequence of $\mathbb{Z}_2$-modules

$$0 \to U'(F_{\mathfrak{p}}) \to Y(F_{\mathfrak{p}}) \to \mathbb{Z}_2 \to 0. \tag{7.7}$$

There is now an obvious commutative diagram with exact rows mapping the sequence (7.6) to the sequence (7.7) in which the left-hand vertical map is obviously surjective, and the middle map is an isomorphism by (7.4). Hence the left vertical map must be an isomoprhism, and the proof is complete. □

We can now prove Proposition 7.1. We have the obvious commutative diagram with exact rows

$$\begin{array}{ccccccccc}
 & & (\bar{C}(F_\infty))_\Gamma & \longrightarrow & (U(F_{\infty,\mathfrak{p}}))_\Gamma & \longrightarrow & (Z(F_\infty))_\Gamma & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bar{C}(F) & \longrightarrow & U'(F_{\mathfrak{p}}) & \longrightarrow & U'(F_{\mathfrak{p}})/\bar{C}(F) & \longrightarrow & 0.
\end{array}$$

Now the left vertical map is surjective by (4.13), and the middle vertical map is an isomorphism by Lemma 7.3, whence the right vertical map must be an isomorphism. This completes the proof of Proposition 7.1.

As before, let $X(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty)$, where $M(F_\infty)$ is the maximal abelian 2-extension of F_∞, which is unramified outside $\mathfrak{p}$. For each $n \geqslant 0$, let $\mathcal{E}(F_n)$ be the group of all global units of F_n, and let $\bar{\mathcal{E}}(F_n)$ be their closure in $U(F_{n,\mathfrak{p}})$ in the $\mathfrak{p}$-adic topology. Define $\bar{\mathcal{E}}(F_\infty) = \varprojlim_n \bar{\mathcal{E}}(F_n)$, where the projective limit is taken with respect to the norm maps. We have already

shown in Theorem 3.8 that F_∞ has no unramified abelian 2-extension. Hence global class field theory provides the following explicit description of $X(F_\infty)$,

$$X(F_\infty) = U(F_{\infty,\mathfrak{p}})/\bar{\mathcal{E}}(F_\infty). \tag{7.8}$$

Finally, define $\bar{\mathcal{E}}'(F) = U'(F_\mathfrak{p}) \cap \bar{\mathcal{E}}(F)$.

PROPOSITION 7.4. *We have $X(F_\infty)^\Gamma = 0$, and $X(F_\infty)_\Gamma = U'(F_\mathfrak{p})/\bar{\mathcal{E}}'(F)$.*

Proof. Let $M(F)$ be the maximal abelian 2-extension of F, which is unramified outside $\mathfrak{p}$. Then

$$X(F_\infty)_\Gamma = \mathrm{Gal}(M(F)/F_\infty) = U'(F_\mathfrak{p})/\bar{\mathcal{E}}'(F).$$

where the first equality is elementary Iwasawa theory, and the second equality is by global class field theory. Obviously the group on the right is finite because $\mathcal{E}'(F)$ has rank 1 as an abelian group. Hence, since $X(F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module by Theorem 3.1, we conclude that we must also have $X(F_\infty)^\Gamma = 0$. □

Define $R(F_\infty) = \bar{\mathcal{E}}(F_\infty)/\bar{C}(F_\infty)$, so that we have the exact sequence of G-modules

$$0 \to R(F_\infty) \to Z(F_\infty) \to X(F_\infty) \to 0. \tag{7.9}$$

COROLLARY 7.5. *We have $(R(F_\infty))_\Gamma = \bar{\mathcal{E}}'(F)/\bar{C}(F)$.*

Proof. Since $(X(F_\infty))^\Gamma = 0$, we have the exact sequence

$$0 \to (R(F_\infty))_\Gamma \to (Z(F_\infty))_\Gamma \to (X(F_\infty))_\Gamma \to 0. \tag{7.10}$$

The corollary then follows immediately from Propositions 7.1 and 7.4. □

Recall that $\Delta = \{1, j\}$ is the Galois group of F_∞ over K_∞. In the group ring $\mathbb{Z}_2[\Delta]$, we define the two elements

$$\epsilon_+ = 1 + j, \ \epsilon_- = 1 - j. \tag{7.11}$$

LEMMA 7.6. *Let $Y = W/V$, with W a $\mathbb{Z}_2[\Delta]$-module and V a submodule. Let ϵ denote either of the above elements (7.11). Then $\epsilon Y = \epsilon W/\epsilon V$.*

Proof. We have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & W & \longrightarrow & Y & \longrightarrow & 0\,, \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \epsilon V & \longrightarrow & \epsilon W & \longrightarrow & \epsilon W/\epsilon V & \longrightarrow & 0 \end{array} \tag{7.12}$$

where the three vertical maps are multiplication by ϵ. Since the middle vertical map is obviously surjective, it follows from the snake lemma that the right vertical map is also surjective, proving the lemma. □

THEOREM 7.7. *For all primes q with $q \equiv 7 \bmod 8$, we have $\epsilon_+ Z(F_\infty) = 0$.*

Proof. It suffices to show that

$$(\epsilon_+ Z(F_\infty))_\Gamma = 0. \tag{7.13}$$

But, since G is commutative, it follows from the previous lemma, Proposition 7.1, and Lemma 7.3 that

$$(\epsilon_+ Z(F_\infty))_\Gamma = \epsilon_+ (Z(F_\infty))_\Gamma = \epsilon_+ U'(F_\mathfrak{p})/\epsilon_+ \bar{C}(F) = 0.$$

This completes the proof. □

THEOREM 7.8. *For all primes q with $q \equiv 7 \bmod 8$, we have $\epsilon_- Z(F_\infty) = \epsilon_- X(F_\infty)$.*

Proof. In view of the exact sequence (7.9) and Lemma 7.6, it suffices to show that $\epsilon_- R(F_\infty) = 0$. Hence it suffices to show that $(\epsilon_- R(F_\infty))_\Gamma = 0$. But, again noting that G is commutative and using Lemma 7.6 and Corollary 7.5, we have

$$(\epsilon_- R(F_\infty))_\Gamma = \epsilon_- (R(F_\infty))_\Gamma = \epsilon_- \bar{\mathcal{E}}'(F)/\epsilon_- \bar{C}(F) = \bar{\mathcal{E}}'(F)^2/\bar{C}(F)^2;$$

the last equality is valid because $j(u) = u^{-1}$ for all u in $\bar{\mathcal{E}}'(F)$. Note also that the group of roots of unit of F is just $\mu_2 = \{\pm 1\}$, because $\mathfrak{p}^*$ is not ramified in F. Hence the conclusion of Theorem 7.8 will be an immediate consequence of the following result. □

PROPOSITION 7.9. *The index of $C(F)$ modulo torsion in $\mathcal{E}'(F)$ modulo torsion is an odd integer.*

The proof is based on the analytic class number formula and Kronecker's limit formula. By Dirichlet's theorem, the unit group of F has rank 1, and, as above, its torsion subgroup is just $\mu_2 = \{\pm 1\}$. Write η for a generator of the unit group of F modulo torsion. We fix an embedding of F into $\mathbb{C}$. If z is any element of F, $|z|_\mathbb{C}$ will denote the square of the ordinary complex absolute value of z. Let h_F denote the class number of F, and, as before, h will denote the class number of K. Let ω denote the non-trivial character of Δ, and write $L(\omega, s)$ for its complex L-series. Then Dirichlet's formula for the residue of the complex zeta functions immediately gives

$$(2\pi)^2 h_F \log |\eta|_\mathbb{C}/|D_F|^{1/2} = 2\pi L(\omega, 1) h/q^{1/2}. \tag{7.14}$$

where D_F denotes the discriminant of F. Now, by Lemma 4.1, the conductor $\mathfrak{f}$ of F/K is equal to $\mathfrak{q}\mathfrak{p}^2$, and so the conductor discriminant formula tells us that $D_F = q^2 N\mathfrak{f}$, where $N\mathfrak{f}$ denotes the absolute norm of $\mathfrak{f}$. Moreover, the functional equation for $L(\omega, s)$ gives that

$$L(\omega, 1) = 2\pi W(\omega) L'(\omega, 0)/(qN\mathfrak{f})^{1/2}, \tag{7.15}$$

where $W(\omega) = \pm 1$ is the sign in the functional equation for $L(\omega, s)$ Combining (7.14) and (7.15), we obtain finally

$$L'(\omega, 0) = W(\omega) \log |\eta|_\mathbb{C} h_F/h. \tag{7.16}$$

We recall that, for each $\alpha \in \mathscr{J}$, the elliptic unit $u_{\alpha,0}$ is defined by $u_{\alpha,0} = N_{\mathfrak{F}_0/F}(\mathfrak{R}_{\alpha,A}(V_0))$. Moreover, by Lemma 7.3, we have $N_{F/K} u_{\alpha,0} = 1$, so that $j(u_{\alpha,0}) = u_{\alpha,0}^{-1}$. Write γ_α for the Artin symbol of the ideal $\alpha\mathcal{O}_K$ in G.

LEMMA 7.10. *For each $\alpha \in \mathscr{J}$, we have $2 \log |u_{\alpha,0}|_\mathbb{C} = (\omega(\gamma_\alpha) - N\alpha) L'(\omega, 0)$.*

Proof. The proof, which we only sketch, rests crucially on Kronecker's second limit formula. For each integral ideal $\mathfrak{g}$ of K, we write $K(\mathfrak{g})$ for the ray class group of K modulo $\mathfrak{g}$. By Lemma 4.1, we know that $K(\mathfrak{g}) = H(A_\mathfrak{g})$ whenever the ideal $\mathfrak{g}$ is divisible by the conductor $\mathfrak{q}$ of ϕ. Now the conductor $\mathfrak{f}$ of ω is equal to $\mathfrak{q}\mathfrak{p}^2$, and so $K(\mathfrak{f})$ is the compositum of its two subfields $\mathfrak{F}_0 = H(A_{\mathfrak{p}^2})$ and $H(A_\mathfrak{q})$. Moreover, $\mathfrak{F}_0 \cap H(A_\mathfrak{q}) = H$ because the primes of H above $\mathfrak{p}$ are totally ramified in $\mathfrak{F}_0$ and unramified in $H(A_\mathfrak{q})$. Thus it is then clear from (4.6) that

$\mathfrak{R}_{\alpha,A}(V_0) = N_{K(\mathfrak{f})/\mathfrak{F}_0} R_{\alpha,A}(V_0 \oplus Q)$, where Q is the primitive $\mathfrak{q}$-division point on A defined by (4.5). Hence we obtain

$$u_{\alpha,0} = N_{K(\mathfrak{f})/F} R_{\alpha,A}(V_0 \oplus Q). \tag{7.17}$$

On the other hand, writing $z_Q = \Omega_\infty(A)/\sqrt{-q}$ and $V_0 = \mathcal{W}(z_0, \mathcal{L})$, we have the fundamental identity (see (5.17))

$$R_{\alpha,A}(V \oplus Q)^{12} = (c_\alpha(A)\theta(z_0 + z_Q, \mathcal{L})^{N\alpha}/\theta(z_0 + z_Q, \alpha^{-1}\mathcal{L}))^{12}.$$

In view of this equality, the classical Kronecker's formula asserts that, for our character ω of $\mathrm{Gal}(K_\mathfrak{f}/K)$, we have

$$(\omega(\gamma_\alpha) - N\alpha)L'(\omega, 0) = \sum_{\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)} \omega(\sigma) \log |\sigma(R_{\alpha,A}(V_0 \oplus Q))|_{\mathbb{C}}. \tag{7.18}$$

Recalling (7.17), we see that the right-hand side of this last formula is simply equal to $\log |u_{\alpha,0}|_{\mathbb{C}} - \log |\tau(u_{\alpha,0})|_{\mathbb{C}}$, where we have written τ for the non-trivial element of $\mathrm{Gal}(F/K)$. But Lemma 7.3 shows that $u_{\alpha,0}.\tau(u_{\alpha,0}) = 1$ (because $u_{\alpha,0}$ is a norm from every finite layer of the $\mathbb{Z}_2$-extension F_∞/F). Hence $\log |u_{\alpha,0}|_{\mathbb{C}} - \log |\tau(u_{\alpha,0})|_{\mathbb{C}} = 2 \log |u_{\alpha,0}|_{\mathbb{C}}$, and so the assertion of the lemma follows from (7.18). This completes the proof. □

For the next lemma, we recall that we have chosen the sign of $\sqrt{-q}$ so that $\mathrm{ord}_\mathfrak{p}((\sqrt{-q} - 1)/2) > 0$.

LEMMA 7.11. *Let $\beta = \sqrt{-q}$. Then $F = K(\sqrt{-\beta})$.*

Proof. The field $K(B_4)$ is an abelian extension of K, whose Galois group is a product of two cyclic groups of order 2, corresponding to the two subfields $F = K(B_{\mathfrak{P}^2})$, and $F^* = K(B_{\mathfrak{P}^{*2}})$, where $\mathfrak{P}^*$ denotes the unramified degree 1 prime of $\mathscr{T}$ above $\mathfrak{p}^*$. Moreover, by the Weil pairing, $K(B_4)$ contains the group μ_4 of fourth roots of unity. Thus we must have $K(B_4) = K(i, \sqrt{b})$, where b is some non-zero element of K, and three quadratic extensions of K contained in $K(B_4)$ are then $K(i), K(\sqrt{b})$, and $K(\sqrt{-b})$. Now the prime $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$ of K does not ramify in $K(i)$, and so, making a choice of the sign of b, we can assume that $F = K(\sqrt{b})$ and $F^* = K(\sqrt{-b})$. Now, by Theorem 2.4, $\mathfrak{q}$ ramifies in both F and F^*, but $\mathfrak{p}^*$ does not ramify in F, and $\mathfrak{p}$ does not ramify in F^*. It follows that we must have $b\mathcal{O}_K = \mathfrak{q}\mathfrak{b}^2$ for some fractional ideal $\mathfrak{b}$ of K. Since the ideal $\mathfrak{q}$ is principal, it follows that $\mathfrak{b}^2$ is principal. But K has odd class number, and so the ideal $\mathfrak{b}$ itself must be principal, whence, modifying b by a square in $K^\times$, we must have $b = \pm\beta$, where, as above $\beta = \sqrt{-q}$. To see which choice of sign to take, we note that

$$\mathrm{ord}_{\mathfrak{p}^*}(-\beta - 1) \geqslant 2,$$

from which it follows easily that $\mathfrak{p}^*$ is unramified in the extension $K(\sqrt{-\beta})$. Hence we must have $F = K(\sqrt{-\beta})$, and the proof of the lemma is complete. □

COROLLARY 7.12. *The curve $A^{(-\beta)}$ has good reduction outside the set of primes of H dividing $\mathfrak{p}$.*

Proof. Due to equation (1.2), we know that all bad primes of $A^{(-\beta)}$ must divide either 2 or 3. However, combining the previous lemma, and Theorem 2.4, we see that every prime of H where $A^{(-\beta)}$ has bad reduction must ramify in the field $\mathfrak{F} = FH$. But the only primes of K which ramify in F are $\mathfrak{q}$ and $\mathfrak{p}$, and so the only primes of H which ramify in $\mathfrak{F}$ must lie above $\mathfrak{p}$ or $\mathfrak{q}$. But the primes of H above $\mathfrak{q}$ are not bad primes because of (1.2), completing the proof. □

We can now complete the proof of Proposition 7.9. It suffices to show that there exists $\alpha \in \mathscr{J}$ such that the index of the subgroup of $\mathcal{E}'(F)$ generated by $u_{\alpha,0}$ is odd. Take $\alpha = a^2 + b^2\sqrt{-q}$, where a is an even positive rational integer which is prime to 3, and b is an odd rational integer which is divisible by 3. Plainly, we then have $(\alpha, 6\mathfrak{f}) = 1$, and $\alpha \equiv 1 \bmod \mathfrak{p}^2$ because $\sqrt{-q} \equiv 1 \bmod \mathfrak{p}^2$. Also, it is clear that α is the norm from F to K of the element $a + b\sqrt{-\beta}$, so that the restriction of the Artin symbol of the ideal $\alpha\mathcal{O}_K$ to $\mathrm{Gal}(F/K)$ is trivial. Noting that $N\alpha \equiv q \bmod 4 \equiv 3 \bmod 4$, we conclude that, for this choice of α, we have

$$N\alpha - \omega(\gamma_\alpha) \equiv 2 \bmod 4.$$

But now, combining this congruence with the formulae of Lemmas (7.16) and (7.10), and recalling that both h_F and h are odd, and $W(\omega) = \pm 1$, we conclude that the index of the subgroup of $C(F)$ generated by $u_{\alpha,0}$ in $\mathcal{E}'(F)$ modulo torsion is indeed odd, and the proof of Proposition 7.9 is complete.

We can now prove the 'main conjecture' for $\epsilon_- X(F_\infty)$. We recall that $\Gamma = \mathrm{Gal}(F_\infty/F)$, and that $\Lambda_{\mathscr{I}}(\Gamma)$ denotes the Iwasawa algebra of Γ with coefficients in $\mathscr{I}$. Write $\rho_{\mathfrak{P},\Gamma}$ for the restriction of $\rho_{\mathfrak{P}}$ to Γ. We recall that, in the results which follow concerning the link between 'main conjectures' and complex L-values, we have fixed until further notice the embedding $\mathfrak{i} : \mathscr{T} \to \mathbb{C}$ given by (2.2).

THEOREM 7.13. *For all primes $q \equiv 7 \bmod 8$, we have the exact sequence of $\Lambda_{\mathscr{I}}(\Gamma)$-modules*

$$0 \to \epsilon_- X(F_\infty)\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to \Lambda_{\mathscr{I}}(\Gamma)/\mu_A\Lambda_{\mathscr{I}}(\Gamma) \to \mathfrak{M}\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to 0, \tag{7.19}$$

where $\mathfrak{M}$ is a finite Γ-module, and μ_A is the unique element of $\Lambda_{\mathscr{I}}(\Gamma)$ such that, for all odd positive integers $k = 1, 3, 5, \ldots$, we have

$$\Omega_\mathfrak{p}(A)^{-k} \int_\Gamma (\rho_{\mathfrak{P},\Gamma})^k d\mu_A = (k-1)!\Omega_\infty(A)^{-k} L(\bar{\phi}^k, k)(1 - \phi^k(\mathfrak{p})/N\mathfrak{p}). \tag{7.20}$$

We note that, since $\Lambda_{\mathscr{I}}(G)$ is the Iwasawa algebra of Γ with coefficients in the group ring $\mathscr{I}[\Delta]$, and $\epsilon_-\mathscr{I}[\Delta] = \epsilon_-\mathscr{I}$, we have

$$\epsilon_-\Lambda_{\mathscr{I}}(G) = \epsilon_-\Lambda_{\mathscr{I}}(\Gamma). \tag{7.21}$$

If m is any element of $\Lambda_{\mathscr{I}}(G)$, we write $m(-)$ for the measure in $\Lambda_{\mathscr{I}}(\Gamma)$ such that $\epsilon_- m = \epsilon_- m(-)$ under the equality (7.21). Now for a character of a p-adic Lie group the integral against a measure of the character coincides with evaluation of the character at the measure, it follows that, for every continuous homomorphism ξ from G to the multiplicative group of $\overline{\mathbb{Q}}_2$ such that $\xi(j) = -1$, we must have

$$\int_G \xi dm = \int_\Gamma \xi_\Gamma dm(-), \tag{7.22}$$

where ξ_Γ denotes the restriction of ξ to Γ. For each $\alpha \in \mathscr{J}$, we recall that γ_α is the Artin symbol of $\alpha\mathcal{O}_K$ in G. We note that in fact γ_α always belongs to Γ because of our hypothesis that $\alpha \equiv 1 \bmod \mathfrak{p}^2$ for α in $\mathscr{I}$. Recall that $\mu_{\alpha,\infty}$ is the measure in $\Lambda_{\mathscr{I}}(G)$ satisfying (5.13).

LEMMA 7.14. *There exists a measure μ_A in $\Lambda_{\mathscr{I}}(\Gamma)$ such that $\mu_{\alpha,\infty}(-) = (N\alpha - \gamma_\alpha)\mu_A$ for all $\alpha \in \mathscr{J}$.*

Proof. Put $v_\alpha = N\alpha - \gamma_\alpha$. Since $v_\alpha \in \Lambda_{\mathscr{I}}(\Gamma)$, it follows easily from (5.13) that, for all $\alpha, \beta \in \mathscr{J}$, we have

$$v_\beta\mu_{\alpha,\infty}(-) = v_\alpha\mu_{\beta,\infty}(-). \tag{7.23}$$

Now we recall that $\Lambda_{\mathscr{I}}(\Gamma)$ is a unique factorization domain, and we claim that we can choose α_0 and β_0 in $\mathscr{J}$ such that v_{α_0} and v_{β_0} are relatively prime. We first choose $\alpha_0 \in \mathscr{J}$ such that

$$\alpha_0 \equiv 1 \bmod \mathfrak{q},\ \alpha_0 \not\equiv 1 \bmod \mathfrak{p}^3,\ \alpha_0 \equiv 1 \bmod (\mathfrak{p}^*)^2,\ \alpha_0 \not\equiv 1 \bmod (\mathfrak{p}^*)^3. \tag{7.24}$$

Thus γ_{α_0} is then a topological generator of Γ, and we can then identify $\Lambda_{\mathscr{I}}(\Gamma)$ with the formal power series ring $\mathscr{I}[[T]]$ by mapping this topological generator to $1+T$, so that $v_{\alpha_0} = N\alpha_0 - (1+T)$. Now choose $\beta_0 \in \mathscr{J}$ such that

$$\beta_0 \equiv 1 \bmod \mathfrak{q},\ \beta_0 \equiv 1 \bmod \mathfrak{p}^3,\ \beta_0 \equiv 1 \bmod (\mathfrak{p}^*)^2,\ \beta_0 \not\equiv 1 \bmod (\mathfrak{p}^*)^3. \tag{7.25}$$

Then we claim that v_{α_0} and v_{β_0} are indeed then relatively prime elements of $\mathscr{I}[[T]]$. To justify this, we note that, provided $\alpha \equiv 1 \bmod \mathfrak{q}$, we have $\phi((\alpha)) = \alpha$, and so γ_α will act on $B_{\mathfrak{P}^\infty}$ by multiplication by α. It follows easily that $\gamma_{\beta_0} = (\gamma_{\alpha_0})^c$, where $c = \log(\beta_0)/\log(\alpha_0)$, where the logarithm is taken in the $\mathfrak{p}$-adic completion of K. Then $v_{\beta_0} = N\beta_0 - (1+T)^c$, and so to show that v_{β_0} and v_{α_0} are relatively prime, one sees immediately that it suffices to show that

$$\log(\beta_0)/\log(\bar{\beta}_0) \neq \log(\alpha_0)/\log(\bar{\alpha_0}), \tag{7.26}$$

where the symbol $\bar{z}$ denotes the complex conjugate of z. But we have $\mathrm{ord}_{\mathfrak{p}}(\log x) = \mathrm{ord}_{\mathfrak{p}}(x-1)$ whenever $\mathrm{ord}_{\mathfrak{p}}(x-1) \geqslant 2$. Thus it follows from (7.24) that $\mathrm{ord}_{\mathfrak{p}}(\log(\alpha_0)/\log(\bar{\alpha_0})) = 0$, whereas (7.25) implies that $\mathrm{ord}_{\mathfrak{p}}(\log(\beta_0)/\log(\bar{\beta}_0)) \geqslant 1$, proving (7.26). Since v_{β_0} and v_{α_0} are relatively prime, it now follows easily from (7.23) that we must have $\mu_{\alpha_0,\infty}(-) = v_{\alpha_0}\mu_A$ for some $\mu_A \in \Lambda_{\mathscr{I}}(\Gamma)$. But then, applying (7.23) again, it follows that $\mu_{\alpha,\infty}(-) = v_\alpha \mu_A$ for all $\alpha \in \mathscr{J}$, and the proof of the lemma is complete. □

We can now prove Theorem 7.13. Since the map j_{F_∞} in (6.8) is a $\Lambda_{\mathscr{I}}(G)$-homomorphism, then recalling (7.21), we see that Theorem 6.4 shows immediately j_{F_∞} gives rise to an exact sequence of $\Lambda_{\mathscr{I}}(\Gamma)$-modules

$$0 \to (\epsilon_- U(F_\infty))\widehat{\otimes}_{\mathcal{O}_{\mathfrak{p}}}\mathscr{I} \to \Lambda_{\mathscr{I}}(\Gamma) \to W\widehat{\otimes}_{\mathcal{O}_{\mathfrak{p}}}\mathscr{I} \to 0, \tag{7.27}$$

where W is some finite Γ-module. Recall that $\bar{C}(F_\infty)$ is, by definition, generated as a $\Lambda(G)$-module by the the norm compatible system of elliptic units $u_{\alpha,\infty}$ defined by (4.14) for α running over $\mathscr{J}$. It then follows from the results of § 5 that $j_{F_\infty}((\epsilon_-\bar{C}(F_\infty))\widehat{\otimes}_{\mathcal{O}_{\mathfrak{p}}}\mathscr{I})$ will be generated as a $\Lambda_{\mathscr{I}}(\Gamma)$-module by the $\mu_{\alpha,\infty}(-)$ for $\alpha \in \mathscr{J}$, which by Lemma 7.14 is equal to the ideal of $\Lambda_{\mathscr{I}}(\Gamma)$ generated by the $v_\alpha\mu_A$ for $\alpha \in \mathscr{J}$, where, as before, $v_\alpha = N\alpha - \gamma_\alpha$. However, we claim that the v_α for $\alpha \in \mathscr{J}$ generate the maximal ideal $(2,T)$ of $\Lambda(\Gamma) = \mathbb{Z}_2[[T]]$. Indeed, the ideal they generate is just the annihilator of the group of all 2-power roots of unity in F_∞, and this group just consists of $\{\pm 1\}$ since the prime $\mathfrak{p}^*$ of K is not ramified in F_∞. Thus we have finally

$$j_{F_\infty}((\epsilon_-\bar{C}(F_\infty))\widehat{\otimes}_{\mathcal{O}_{\mathfrak{p}}}\mathscr{I}) = (2\mathscr{I}, T)\mu_A. \tag{7.28}$$

On combining (7.27) and (7.28), noting that $\epsilon_- Z(F_\infty) = \epsilon_- U(F_\infty))/\epsilon_-\bar{C}(F_\infty)$, and recalling that $\epsilon_- X(F_\infty)$ has no non-zero finite subgroup by Lemma 3.6, we conclude from Theorem 7.8 that the exact sequence (7.19) is valid. Moreover, applying (7.22) with $\xi = (\rho_{\mathfrak{P}})^k (k = 1,3,5,\ldots)$, we obtain (7.20) from (5.13).

Corollary 7.15. *Assume $q \equiv 7 \bmod 16$. Then, for all complex characters χ of finite order of G with $\chi(j) = 1$, we have $L(\rho\chi, 1) \neq 0$.*

Proof. Since $q \equiv 7 \bmod 16$, we have $\epsilon_- X(F_\infty) = 0$ by Theorem 3.1, and so it follows from the exact sequence (7.19) that μ_A must be a unit in the Iwasawa algebra $\Lambda_{\mathscr{I}}(\Gamma)$. Hence $\int_\Gamma (\rho_{\mathfrak{P}}\chi)_\Gamma d\mu_A$ will be a unit in $\mathscr{I}$, and so, noting that $L(\overline{\rho\chi}, 1)$ is the complex

conjugate of $L(\rho\chi, 1)$, the result follows from the theorem in the Appendix and the fact that $(\rho_{\mathfrak{P}}\chi)(j) = -1$. □

Similarly, we have

$$\epsilon_+\Lambda_{\mathscr{I}}(G) = \epsilon_+\Lambda_{\mathscr{I}}(\Gamma). \tag{7.29}$$

If m is any element of $\Lambda_{\mathscr{I}}(G)$, we write $m(+)$ for the measure in $\Lambda_{\mathscr{I}}(\Gamma)$ such that $\epsilon_+ m = \epsilon_+ m(+)$ under the equality (7.29). For every continuous homomorphism ξ from G to the multiplicative group of $\overline{\mathbb{Q}}_2$ such that $\xi(j) = +1$, we then have

$$\int_G \xi dm = \int_\Gamma \xi_\Gamma dm(+), \tag{7.30}$$

where ξ_Γ denotes the restriction of ξ to Γ. Now exactly the same proof as in Lemma 7.14 shows that there exists ν_A in $\Lambda_{\mathscr{I}}(\Gamma)$ such that

$$\mu_{\alpha,\infty}(+) = (N\alpha - \gamma_\alpha)\nu_A \tag{7.31}$$

for all $\alpha \in \mathscr{J}$. Moreover, as before, we have the exact sequence

$$0 \to (\epsilon_+ U(F_\infty))\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to \Lambda_{\mathscr{I}}(\Gamma) \to W\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I} \to 0, \tag{7.32}$$

where again W is some finite $\Lambda(\Gamma)$-module. Again we have

$$j_{F_\infty}((\epsilon_+\bar{C}(F_\infty))\widehat{\otimes}_{\mathcal{O}_\mathfrak{p}}\mathscr{I}) = (2\mathscr{I}, T)\nu_A. \tag{7.33}$$

THEOREM 7.16. *For all primes q with $q \equiv 7 \bmod 8$, the measure ν_A is a unit in $\Lambda_{\mathscr{I}}(\Gamma)$.*

Proof. This follows immediately from combining (7.32) and (7.33), noting that $\epsilon_+ Z(F_\infty) = \epsilon_+ U(F_\infty)/\epsilon_+\bar{C}(F_\infty)$, and then using Theorem 7.7. □

COROLLARY 7.17. *Assume $q \equiv 7 \bmod 8$. Then, for all complex characters χ of finite order of G with $\chi(j) = -1$, we have $L(\rho\chi, 1) \neq 0$.*

Proof. We simply apply (7.30) with $\xi = \rho_{\mathfrak{P}}\chi$, and $m = \mu_{\alpha,\infty}$, noting that $(\rho_{\mathfrak{P}}\chi)(j) = +1$. Since ν_A is a unit in $\Lambda_{\mathscr{I}}(\Gamma)$, $\int_\Gamma (\rho_{\mathfrak{P}}\chi)_\Gamma d\nu_A$ will be a unit in $\mathscr{I}$, and we then finally apply the theorem in the Appendix to give the value of $\int_G \xi d\mu_{\alpha,\infty}$. □

COROLLARY 7.18. *Assume $q \equiv 7 \bmod 8$, and recall that $F = K(\sqrt{-\beta})$, where $\beta = \sqrt{-q}$. Let $B^{(-\beta)}$ denote the twist of the abelian variety B by the quadratic extension F/K, and let $\rho_{B^{(-\beta)}}$ be its Serre–Tate Grossencharacter. Then $\rho_{B^{(-\beta)}}$ has bad reduction only at the prime $\mathfrak{p}$, and $L(\rho_{B^{(-\beta)}}\eta, 1) \neq 0$, where η is any complex character of finite order of $\mathrm{Gal}(K_\infty/K)$.*

Proof. We have $\rho_{B^{(-\beta)}} = \rho\omega$, where ω again denotes the non-trivial character of Δ. It is readily verified that $\mathfrak{q}$ does not divide the conductor of $\rho\omega$, whence $B^{(-\beta)}$ will have good reduction at $\mathfrak{q}$. The final assertion then follows from Corollary 7.17, on noting that we have $(\omega\eta)(j) = -1$. □

Now, as in the Introduction, let $\mathfrak{M}_K$ denote the set of all non-zero integers M in $\mathcal{O}_K$, which are prime to q, satisfy $M \equiv 1 \bmod 4$, and are not squares in K. For each $M \in \mathfrak{M}_K$, let $B^{(M)}$ be the abelian variety defined over K which is the twist of B by the quadratic extension $K(\sqrt{M})/K$, and let $\rho_{B^{(M)}}$ be the Serre–Tate character of $B^{(M)}$. For each $n \geqslant 0$, let $F(M)_n$ be the field obtained by adjoining to K the coordinates of the $\mathfrak{P}^{n+2}$-division points of $B^{(M)}$. Since $B^{(M)}$ has good reduction at $\mathfrak{p}$ because $M \equiv 1 \bmod 4$, it is easily seen that $[F(M)_n : K] = 2^{n+1}$,

and that $F(M)_n$ is a quadratic extension of the field K_n for all $n \geqslant 0$. As usual, for each $n \geqslant 0$, we write $N_{F(M)_n/K}$ and $N_{K_n/K}$ for the norm maps for the extensions $F(M)_n/K$ and K_n/K.

THEOREM 7.19. *Assume that $q \equiv 7 \bmod 8$, and that $M \in \mathfrak{M}_K$. Then, for all $n \geqslant 0$, we have $\mathrm{ord}_{s=1} L(\rho_{B^{(M)}} \circ N_{F(M)_n/K}, s) = \mathrm{ord}_{s=1} L(\rho_{B^{(M)}} \circ N_{K_n/K}, s)$. Moreover the $\mathbb{Z}$-rank of $B^{(M)}(F(M)_n)$ = the $\mathbb{Z}$-rank of $B^{(M)}(K_n)$ for all $n \geqslant 0$.*

Proof. To lighten the notation, write $\mathfrak{B} = B^{(M)}$. An entirely similar argument to that given in the proof of Theorem 2.4 shows that $\mathfrak{B}$ has good reduction everywhere over the field $F(M)_0 = K(\mathfrak{B}_{\mathfrak{P}^2})$. Now, since $F = K(\sqrt{-\beta})$ by Lemma 7.11, and $\mathfrak{B}$ is isomorphic to B over the field $K(\sqrt{M})$, we see that $F(M)_0$ must be one of the three quadratic extensions of K contained in the field $K(\sqrt{-\beta}, \sqrt{M})$. But, since $\mathfrak{B}$ has good reduction everywhere over the field $F(M_0)$, and the set of bad primes of $\mathfrak{B}$ over K consists of $\mathfrak{q}$ and the primes of K dividing M, all of these bad primes must necessarily ramify in $F(M)_0$, whence $F(M)_0 = K(\sqrt{-\beta M})$. In particular, writing $\mathfrak{B}^{(-\beta M)}$ for the twist of $\mathfrak{B}$ by the quadratic extension $F(M)_0$, it follows that

$$\rho_{\mathfrak{B}} \circ N_{F(M)_0/K} = \rho_{\mathfrak{B}} \rho_{\mathfrak{B}^{(-\beta M)}}. \tag{7.34}$$

But, since $\mathfrak{B} = B^{(M)}$, we must have $\mathfrak{B}^{(-\beta M)} = B^{(-\beta)}$, whence

$$\rho_{\mathfrak{B}} \circ N_{F(M)_0/K} = \rho_{\mathfrak{B}} \rho_{B^{(-\beta)}}. \tag{7.35}$$

Since $L(\rho_{B^{(-\beta)}} \circ N_{K_n/K}, s) = \prod_\eta L(\rho_{B^{(-\beta)}} \eta, s)$, where the product is taken over all 2^n complex characters η of finite order of $\mathrm{Gal}(K_n/K)$, the first conclusion of Theorem 7.19 follows from Corollary 7.18. The proof of the second assertion of Theorem 7.19 is entirely parallel to that given for Theorem 3.12 in § 3, and we omit the detailed arguments. □

Finally, we note that the proofs we have given in § 5 and above are valid for every choice of the embedding $\mathfrak{i} : \mathscr{T} \to \mathbb{C}$ made at the beginning of § 2. In fact, there are precisely h such embeddings lying above our fixed embedding of K in $\mathbb{C}$, and we now denote these distinct embeddings by $i^{(r)}$ $(r = 1, \ldots, h)$. Let $\rho^{(r)}$ denote the complex Grossencharacter of B/K relative to the embedding $\mathfrak{i}^{(r)}$, and let $\psi_{A/H}$ denote the complex Grossencharacter of the elliptic curve A/H. Then we have

$$L(\psi_{A/H}, s) = \prod_{r=1}^{h} L(\rho^{(r)}, s). \tag{7.36}$$

Since Corollaries 7.15 and 7.17 holds for each of the $\rho^{(r)}$ $(r = 1, \ldots, h)$, the assertion of Theorem 1.1 follows easily. By an entirely similar argument, one shows that Theorem 1.5 follows from Corollary 7.18. Finally, recalling that Corollary 7.18 and Theorem 7.19 are valid for all primes $q \equiv 7 \bmod 8$, it is also clear that Theorem 1.7 follows from Theorem 7.19 by an analogous argument.

Finally, for the proof of Theorem 1.2, we note that, writing $L(A/J, s)$ for the complex L-series of a finite extension J of H, Theorem 1.1 tells us that, when $q \equiv 7 \bmod 16$, we have $L(A/J, 1) \neq 0$ whenever $J \subset \mathfrak{F}_\infty$. But then a standard argument, whose details we omit, shows that the finiteness of both $A(J)$ and $Ш(A/J)(\mathfrak{p})$ follow from this non-vanishing result and the main conjecture for $A/\mathfrak{F}_\infty$, which is proven in [**10**].

8. *Related results*

Combining Theorems (3.1) and (3.9), we have shown in § 3 that, for all primes $q \equiv 7 \bmod 16$, we have $\mathrm{Sel}_{\mathfrak{P}^\infty}(B/F_\infty) = 0$, where we recall that $F_\infty = K(B_{\mathfrak{P}^\infty})$. However, the following theorem

shows that nothing like this is valid for the $\mathfrak{p}^\infty$-Selmer group of the elliptic curve A over the field

$$\mathfrak{F}_\infty = H(A_{\mathfrak{p}^\infty}) = HF_\infty. \tag{8.1}$$

If L is any algebraic extension of H, we write $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/L)$ for the classical $\mathfrak{p}^\infty$-Selmer group of A/L. We also write $M(\mathfrak{F}_\infty)$ for the maximal abelian 2-extension of $\mathfrak{F}_\infty$, which is unramified outside the primes of $\mathfrak{F}_\infty$ lying above $\mathfrak{p}$, and put $X(\mathfrak{F}_\infty) = \mathrm{Gal}(M(\mathfrak{F}_\infty)/\mathfrak{F}_\infty)$. Since A has good reduction everywhere over $\mathfrak{F}_\infty$ by Theorem (2.4), we have

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty) = \mathrm{Hom}(X(\mathfrak{F}_\infty), A_{\mathfrak{p}^\infty}). \tag{8.2}$$

THEOREM 8.1. *Assume $q \equiv 7 \bmod 16$. Then, provided there is more than one prime of H lying above $\mathfrak{p}$, or equivalently provided the ideal class of $\mathfrak{p}$ does not have order exactly equal to h, we have $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty) = Ш(A/\mathfrak{F}_\infty)(\mathfrak{p}) = (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})^{m_q}$, for some integer $m_q > 0$.*

Proof. We recall that $H_\infty = HK_\infty$. Let $M(H_\infty)$ be the maximal abelian 2-extension of H_∞ which is unramified outside the primes of H_∞ above $\mathfrak{p}$, and write $X(H_\infty) = \mathrm{Gal}(M(H_\infty)/H_\infty)$. It is proven in [**6**] that $X(H_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module. By entirely similar arguments, based on Nakayama's Lemma, to those given in Section 3, one can then show that $X(\mathfrak{F}_\infty)$ is also a free finitely generated $\mathbb{Z}_2$-module. It follows from (8.2) that $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty)$ is a direct sum of a finite number of copies of $K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$. Since Theorem 1.2 proves that $A(\mathfrak{F}_\infty)$ is a torsion group, to complete the proof it suffices to show that $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty) \neq 0$, which is equivalent to showing that

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty)^\Gamma \neq 0, \tag{8.3}$$

where we are now using the symbol Γ for $\mathrm{Gal}(\mathfrak{F}_\infty/\mathfrak{F})$. If L is any algebraic extension of H, we define the modified Selmer group

$$\mathrm{Sel}'_{\mathfrak{p}^\infty}(A/L) = \mathrm{Ker}\left(H^1(L, A_{\mathfrak{p}^\infty}) \to \prod_{v \nmid \mathfrak{p}} H^1(L_v, A)(\mathfrak{p}) \right), \tag{8.4}$$

where now the product is taken over all primes v of L which do not lie above the prime $\mathfrak{p}$ of K. Since A has good reduction everywhere over the field $\mathfrak{F}$, and the extension $\mathfrak{F}_\infty/\mathfrak{F}$ is unramified outside $\mathfrak{p}$, entirely similar arguments to those given in the proofs of Theorem 3.9 and Proposition 3.11 show that $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty) = \mathrm{Sel}'_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty)$, and that

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty)^\Gamma = \mathrm{Sel}'_{\mathfrak{p}^\infty}(A/\mathfrak{F}). \tag{8.5}$$

Now we have the obvious exact sequence

$$0 \to \mathrm{Sel}_{\mathfrak{p}^\infty}(A/\mathfrak{F}) \to \mathrm{Sel}'_{\mathfrak{p}^\infty}(A/\mathfrak{F}) \to \prod_{w|\mathfrak{p}} H^1(\mathfrak{F}_w, A)(\mathfrak{p}), \tag{8.6}$$

where w runs over the places of $\mathfrak{F}$ dividing $\mathfrak{p}$. Denoting the right-hand map in this last exact sequence by g, the work of Cassels–Poitou–Tate (see, for example, Corollary 4 of the Appendix of [**27**]) gives the following exact description of the cokernel of g. Let π now denote a non-zero element of $\mathcal{O}_K$, such that $\pi\mathcal{O}_K = \mathfrak{p}^r$ for some integer $r \geqslant 1$, and let π^* denote the complex conjugate of π. By Tate local duality, $H^1(\mathfrak{F}_w, A)(\mathfrak{p})$ is dual to $\varprojlim_n A(\mathfrak{F}_w)/\pi^{*n}A(\mathfrak{F}_w)$, and this latter group is easily seen to be isomorphic to $\tilde{A}_w(k_w)(\mathfrak{p}^*)$, where $\tilde{A}_w$ denotes the reduction of A modulo w, and k_w is the residue field of w. Define

$$\mathfrak{S}_{\mathfrak{p}^{*\infty}} = \varprojlim_n \mathrm{Sel}_{\pi^{*n}}(A/\mathfrak{F}), \tag{8.7}$$

where $\mathrm{Sel}_{\pi^{*n}}(A/\mathfrak{F})$ denotes the classical Selmer group of $A/\mathfrak{F}$ relative to the endomorphism π^{*n} of A. Now by Theorem 1.1, we have $L(A/\mathfrak{F},1) \neq 0$, and we have already noted in Theorem 1.2 that this implies that $A(\mathfrak{F})$ and $Ш(A/\mathfrak{F})(\mathfrak{p})$ are both finite. Then analogous arguments to those used to prove Corollary 16 in [27] for split odd primes p will also enable one to show that, even for $p = 2$, the finiteness of $Ш(A/\mathfrak{F})(\mathfrak{p})$ implies in turn the finiteness of $Ш(A/\mathfrak{F})(\mathfrak{p}^*)$. Alternatively, we could use the main conjecture for A over the $\mathbb{Z}_2$-extension $\mathfrak{F}K^*_\infty/\mathfrak{F}$, where K^*_∞ is the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}^*$, to show that the non-vanishing of $L(A/\mathfrak{F},1)$ implies the finiteness of $Ш(A/\mathfrak{F})(\mathfrak{p}^*)$. It then follows easily that we have

$$\mathfrak{S}_{\mathfrak{p}^*\infty} = A(\mathfrak{F})(\mathfrak{p}^*). \tag{8.8}$$

But $A(\mathfrak{F})(\mathfrak{p}^*) = A_{\mathfrak{p}^*}$ because the primes of H above $\mathfrak{p}^*$ are unramified in $\mathfrak{F}$. Further, we note that $\tilde{A}_w(k_w)(\mathfrak{p}^*) \neq 0$ for every prime w of $\mathfrak{F}$ above $\mathfrak{p}$, since reduction modulo w is injective on $A_{\mathfrak{p}^*}$. Putting all together, the theorem of Cassels, Tate, and Poitou shows finally that the cokernel of the map g is dual to the image of the natural injection

$$A_{\mathfrak{p}^*} \to \prod_{w|\mathfrak{p}} \tilde{A}_w(k_w)(\mathfrak{p}^*). \tag{8.9}$$

In particular, we see that the cokernel of g has order exactly 2. Finally, we note that $\tilde{A}_w(k_w)(\mathfrak{p}^*) \neq 0$ for every prime w of $\mathfrak{F}$ above $\mathfrak{p}$, since reduction modulo w is injective on $A_{\mathfrak{p}^*}$. Hence $\prod_{w|\mathfrak{p}} H^1(\mathfrak{F}_w, A)(\mathfrak{p})$ will always have order strictly greater than the cokernel of the map g when there is more than one prime w of H above $\mathfrak{p}$. This shows that $\mathrm{Sel}'_{\mathfrak{p}^\infty}(A/\mathfrak{F}_\infty) \neq 0$, when there is more than one prime of H above $\mathfrak{p}$, and the proof of the theorem is complete. □

We note that Theorems 3.1 and 3.9 show that $Ш(B/F_\infty)(\mathfrak{P}) = 0$ when $q \equiv 7 \bmod 16$. However, when there is more than one prime of H above $\mathfrak{p}$, this seems in contrast with the fact that $Ш(A/\mathfrak{F}_\infty)(\mathfrak{p})$ is a divisible group of strictly positive $\mathbb{Z}_2$-corank. We are grateful to Milne for the following comment about this situation. Let $\mathfrak{L}/L$ be any finite Galois extension of subfields of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, let $\mathfrak{J}$ be any abelian variety defined over $\mathfrak{L}$, and let J be the restriction of scalars of $\mathfrak{J}$ from $\mathfrak{L}$ to L. Then the $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$-module $J(\overline{\mathbb{Q}})$ is the induced representation of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathfrak{L})$-module $\mathfrak{J}(\overline{\mathbb{Q}})$, and similarly at the completions at all places of L. Hence the local and global Galois cohomology groups of these representations coincide. It follows, in particular, that $Ш(\mathfrak{J}/\mathfrak{L}) = Ш(J/L)$. Thus, applying this remark to the extension $\mathfrak{F}_\infty/F_\infty$, we conclude that $Ш(A/\mathfrak{F}_\infty) = Ш(B/F_\infty)$. This also implies that the endomorphism ring $\mathscr{B}$ of B/K operates on $Ш(A/\mathfrak{F}_\infty)$, and so in particular, we have

$$Ш(A/\mathfrak{F}_\infty)(\mathfrak{p}) = \oplus_{\mathfrak{Q}|\mathfrak{p}} Ш(A/\mathfrak{F}_\infty)(\mathfrak{Q}), \tag{8.10}$$

where now $\mathfrak{Q}$ runs through all the primes of $\mathscr{T}$ lying above the prime $\mathfrak{p}$ of K. Note also that all primes of $\mathscr{T}$ above $\mathfrak{p}$ are unramified because of result of Gross mentioned in § 2 and the fact that h is odd. Moreover, $\mathfrak{P}$ is the unique annihilator of $A_{\mathfrak{p}} = B(K)_{\mathfrak{p}}$ lying inside $\mathscr{T}$, so that all the primes of $\mathfrak{Q}$ of $\mathscr{T}$ lying above $\mathfrak{p}$ and distinct from $\mathfrak{P}$ must have residue field strictly bigger than $\mathbb{F}_2$. Hence the arguments of § 2 cannot be applied to show that $Ш(A/\mathfrak{F}_\infty)(\mathfrak{Q}) = 0$ when $\mathfrak{Q} \neq \mathfrak{P}$. Moreover, if we assume that there is more than one prime of H above $\mathfrak{p}$, we certainly have $H \neq K$, and thus there is at least one prime $\mathfrak{Q}$ of $\mathscr{T}$, distinct from $\mathfrak{P}$, above $\mathfrak{p}$. Theorem 8.1 then proves that we must have $Ш(A/\mathfrak{F}_\infty)(\mathfrak{Q}) \neq 0$ for at least one prime $\mathfrak{Q}$ of $\mathscr{T}$ above $\mathfrak{p}$ and distinct from $\mathfrak{P}$.

Finally, we record without proof a special case of an old result of Wiles and the first author [13] (cf. [13, Theorem 11], but note that the proof given there assumes $p > 2$, so that one has to rework the argument slightly to handle the case $p = 2$). Let $M(F)$ denote the maximal abelian 2-extension of F unramified outside the unique prime of F lying above $\mathfrak{p}$. Obviously $M(F) \supset F_\infty$, and it is a nice exercise in global class field theory to show that $[M(F) : F_\infty]$

is finite, and establish the following exact formula for this degree. One also has to use the fundamental fact proven earlier (Theorem 3.8) that F always has odd class number.

THEOREM 8.2. *Assume that $q \equiv 7 \bmod 8$. Let v denote the unique prime of F lying above $\mathfrak{p}$, and let $\log_v$ denote the v-adic logarithm. Then*

$$[M(F) : F_\infty] = 2^t, \text{ where } t = (\mathrm{ord}_v(\log_v(\eta)) - 2)/2, \tag{8.11}$$

and η is any generator of the unit group of F modulo torsion.

Since $X(F_\infty)_\Gamma = Gal(M(F)/F_\infty)$, we obtain as an immediate corollary of (8.11) and Theorem 3.1:

COROLLARY 8.3. *When the prime q satisfies $q \equiv 7 \bmod 16$, we always have $\mathrm{ord}_v(\log_v(\eta)) = 2$.*

We are extremely grateful to Zhibin Liang for having computed for us the fundamental unit η and $\mathrm{ord}_v(\log_v(\eta))$ for all primes $q \equiv 15 \bmod 16$ with $q < 2500$. In particular, when combined with Theorem 8.2, Liang's calculations gave strong numerical evidence that $X(F_\infty) \neq 0$ for all primes $q \equiv 15 \bmod 16$. We have to confess that we cannot see how to prove this last statement using the techniques of Iwasawa theory. However, recently Jianing Li [**25**] of the University of Science and Technology, Hefei, has discovered an ingenious elementary proof of both Corollary 8.3 and the fact that $\mathrm{ord}_v(\log_v(\eta)) \geqslant 4$ when $q \equiv 15 \bmod 16$. Thus, for all primes $q \equiv 15 \bmod 16$, Li's result combined with (8.11) shows that $M(F) \neq F_\infty$, and so, since $X(F_\infty)_\Gamma = Gal(M(F)/F_\infty)$, it follows from Nakayama's lemma that $X(F_\infty) \neq 0$, which in turn implies that $X(F_\infty)$ has positive $\mathbb{Z}_2$-rank by Theorem 3.1.

9. *Zhao's method*

In this section, we prove Theorem 1.3 using Zhao's method [**31, 32**]. As in the Introduction, $\mathscr{R}$ will denote the set of all square free positive integers R of the form $R = r_1 \dots r_k$, where $k \geqslant 0$, and $r_1, \dots, r_k$ are distinct primes such that (i) $r_i \equiv 1 \bmod 4$, and (ii) r_i is inert in K, for $i = 1, \dots, k$. For the rest of this section, R will denote an arbitrary element of $\mathscr{R}$. For each positive divisor $d > 1$ of R, we let χ_d be the non-trivial character of $\mathrm{Gal}(K(\sqrt{d})/K)$, and we define $\phi_d = \phi\chi_d$, where, as always, ϕ denotes the Hecke character attached to the abelian variety B/K which is the restriction of scalars of A from H to K. We also put $\phi_1 = \phi$. Recall that $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$ is the conductor of ϕ. We recall that $i : \mathscr{T} \to \mathbb{C}$ is any embedding which extends our given embedding of K into $\mathbb{C}$, so that we can view all of the Hecke characters ϕ_d as being complex valued.

LEMMA 9.1. *For each positive divisor d of R, the Hecke character ϕ_d has conductor $d\mathfrak{q}$. Moreover, if r is any prime dividing R, which does not divide d, then $\phi_d(r\mathcal{O}_K) = -r$.*

Proof. The positive integer d is square free, and satisfies $d \equiv 1 \bmod 4$ since each prime dividing d is $\equiv 1 \bmod 4$, from which it follows that χ_d has conductor $d\mathcal{O}_K$. But ϕ has conductor $\mathfrak{q}$, which is prime to $d\mathcal{O}_K$, and thus ϕ_d will have conductor $d\mathfrak{q}$. Let $\mathfrak{r} = r\mathcal{O}_K$. Since $-r$ is a square modulo q, and h is odd, the explicit formula for ϕ given at the beginning of [**3**, § 2] shows that $\phi(\mathfrak{r}) = -r$. On the other hand, since r is inert in K, and the Galois group of $K(\sqrt{d})/\mathbb{Q}$ is not cyclic when $d > 1$, the prime $\mathfrak{r}$ of K must split in $K(\sqrt{d})$, and so we must have $\chi_d(\mathfrak{r}) = 1$, whence the second assertion of the lemma follows. □

For each positive divisor d of R, let $A^{(d)}$ be the twist of A by the extension $H(\sqrt{d})/H$ and $B^{(d)}$ the twist of B by the extension $K(\sqrt{d})/K$. Then $B^{(d)}$ is the restriction of scalars from H to K of $A^{(d)}$, and $B^{(d)}$ has Hecke character ϕ_d. Recall that ω denotes the Néron differential of our global minimal equation (2.3) of A/H, and that its complex period lattice is $\mathcal{L} = \Omega_\infty(A)\mathcal{O}_K$. Gross has shown in [22] (see Proposition 4.3) that the differential $\omega/\sqrt{d}$ on $A/H(\sqrt{d})$ descends to a global minimal differential on $A^{(d)}/H$ which we denote by $\omega(d)$. The following lemma is then clear from Gross' result and [19, Proposition 4.10, (vi)].

LEMMA 9.2. *For each positive divisor d of R, the complex period lattice of $\omega(d)$ is equal to $\Omega_\infty(A)\mathcal{O}_K/\sqrt{d}$. Let $E = A^{(d)}$, and, for each integral ideal $\mathfrak{a}$ of K prime to $R\mathfrak{q}$, let $E^{\mathfrak{a}}$ be the curve obtained by applying the Artin symbol of $\mathfrak{a}$ to the coefficients of the global minimal equation for E, and let $\omega(d)_{\mathfrak{a}}$ be the Néron differential of $E^{\mathfrak{a}}$. Then we have $\eta_E(\mathfrak{a})^*(\omega(d)_{\mathfrak{a}}) = \xi_d(\mathfrak{a})\omega(d)$, where $\xi_d(\mathfrak{a}) = \xi(\mathfrak{a})/\chi_d(\mathfrak{a})$.*

Let $\mathfrak{a}$ be any integral ideal of K with $(\mathfrak{a}, R\mathfrak{q}) = 1$, and, as before, let $\gamma_{\mathfrak{a}}$ denote the ideal class of $\mathfrak{a}$. Always assuming that d is a positive divisor of R, we define the imprimitive partial Hecke L-series

$$L_{R\mathfrak{q}}(\overline{\phi_d}, \gamma_{\mathfrak{a}}, s) = \sum_{(\mathfrak{b}, R\mathfrak{q})=1, \mathfrak{b}\in\gamma_{\mathfrak{a}}} \frac{\overline{\phi_d}(\mathfrak{b})}{N(\mathfrak{b})^s}, \tag{9.1}$$

where the sum on the right is taken over all integral ideals $\mathfrak{b}$ of K, which are prime to $R\mathfrak{q}$, and which lie in the class $\gamma_{\mathfrak{a}}$. It is classical that the Dirichlet series on the right converges for $R(s) > 3/2$, and it has a holomorphic continuation to the whole complex plane. We recall a classical formula for $L_{R\mathfrak{q}}(\overline{\phi_d}, \gamma_{\mathfrak{a}}, 1)$, which essentially goes back to the nineteenth 19th century (see [19]). Recall that, for any lattice $\mathscr{L}$, $\mathcal{E}_1^*(z, \mathscr{L}) = H_1(z, 1, \mathscr{L})$ is the Eisenstein series of weight 1 defined earlier. We write $K(R\mathfrak{q})$ for the ray class field of K modulo $R\mathfrak{q}$, and let $\mathrm{Tr}_{K(R\mathfrak{q})/H}$ be the trace map from $K(R\mathfrak{q})$ to H.

PROPOSITION 9.3. *Assume $R \in \mathscr{R}$, and let d be any positive divisor of R. Then, for all integral ideals $\mathfrak{a}$ of K, which are prime to $R\mathfrak{q}$, we have*

$$\frac{\phi_d(\mathfrak{a})R\sqrt{-qd}}{\xi_d(\mathfrak{a})} \cdot \frac{L_{R\mathfrak{q}}(\overline{\phi}_d, \gamma_{\mathfrak{a}}, 1)}{\Omega_\infty(A)} = \mathrm{Tr}_{K(R\mathfrak{q})/H}\left(\mathcal{E}_1^*\left(\frac{\xi_d(\mathfrak{a})\Omega_\infty(A)}{R\sqrt{-qd}}, \frac{1}{\sqrt{d}}\mathcal{L}_{\mathfrak{a}}\right)\right). \tag{9.2}$$

Proof. We apply [19, Proposition 5.5] to the curve $E = A^{(d)}$ over the field H, with $\mathfrak{g} = R\mathfrak{q}$, and $\rho = \Omega_\infty(A)/(R\sqrt{-qd})$. Since the conductor of the Grossencharacter ϕ_d is equal to $d\mathfrak{q}$ by Lemma 9.1, the obvious analogue of Lemma 4.1 shows that $H(E_{\mathfrak{g}})$ is equal to the ray class field $K(R\mathfrak{q})$. Moreover, we have $\eta_E(\mathfrak{a})^*(\omega(d)_{\mathfrak{a}}) = \xi_d(\mathfrak{a})\omega(d)$ by Lemma 9.2. It then follows from [19, Proposition 5.5] that

$$\frac{\phi_d(\mathfrak{a})R\sqrt{-qd}}{\xi_d(\mathfrak{a})} \cdot \frac{L_{R\mathfrak{q}}(\overline{\phi}_d, \gamma_{\mathfrak{a}}, 1)}{\Omega_\infty(A)} = \sum_{\mathfrak{b}\in\mathfrak{B}} \mathcal{E}_1^*\left(\frac{\phi_d(\mathfrak{b})\xi_d(\mathfrak{a})\Omega_\infty(A)}{R\sqrt{-qd}}, \frac{1}{\sqrt{d}}\mathcal{L}_{\mathfrak{a}}\right), \tag{9.3}$$

where $\mathfrak{B}$ denotes any set of integral prime ideals of K, prime to $R\mathfrak{q}$, whose Artin symbols in $\mathrm{Gal}(K(R\mathfrak{q})/K)$ give precisely $\mathrm{Gal}(K(R\mathfrak{q})/H)$, and, as in § 4, $\mathcal{L}_{\mathfrak{a}} = \xi(\mathfrak{a})\Omega_\infty(A)\mathfrak{a}^{-1}$. However, by [19, Theorem 6.2], we note that, since the Artin symbol of every ideal $\mathfrak{b} \in \mathfrak{B}$ fixes the field of definition H of E, the right-hand side of (9.3) is none other than the right-hand side of (9.2). This completes the proof. □

We now introduce the two fields

$$J_R = K(\sqrt{r_1}, \ldots, \sqrt{r_k}), \;\; H_R = H(\sqrt{r_1}, \ldots, \sqrt{r_k}), \tag{9.4}$$

where, as always, the r_i, $1 \leqslant i \leqslant k$, are the distinct prime factors of R.

LEMMA 9.4. *We have $J_R \cap H = K$, $[H_R : J_R] = h$, and $H_R \subset K(R\mathfrak{q})$. Moreover, for each positive divisor d of R, $B^{(d)}$ is isomorphic to B over J_R, and $A^{(d)}$ is isomorphic to A over H_R.*

Proof. Since the class number h is odd, and $[J_R : K] = 2^k$ by Kummer theory, it follows that $J_R \cap H = K$. Moreover, the extension $K(\sqrt{r_i})/K$ has conductor $r_i\mathcal{O}_K$ since $r_i \equiv 1 \bmod 4$, and thus this extension is a subfield of $K(R\mathfrak{q})$. The final assertion of the lemma is also clear since J_R contains $\sqrt{d}$. □

It follows from (9.3) that, for each divisor d of R, the partial L-value $\sqrt{d}L_{R\mathfrak{q}}(\overline{\phi}_d, \gamma_{\mathfrak{a}}, 1)/\Omega_\infty(A)$ belongs to the compositum of fields $H\mathscr{T}$. Recall that $\mathfrak{P}$ is our degree one prime of $\mathscr{T}$ above $\mathfrak{p}$. Take any prime v of $H_R\mathscr{T}$ lying above the prime $\mathfrak{P}$ of $\mathscr{T}$. We also assume R is fixed for the limit arguments which follow. For each $n \geqslant 0$, let $\mathscr{C}_n$ be a set of integral ideals of K, prime to $R\mathfrak{q}$, whose Artin symbols in $\mathrm{Gal}(H_R(A_{\mathfrak{p}^{n+2}})/K))$ give precisely $\mathrm{Gal}(H_R(A_{\mathfrak{p}^{n+2}})/J_R(B_{\mathfrak{P}^{n+2}}))$. One sees easily that, for each $n \geqslant 0$, $\mathscr{C}_n$ gives a complete set of representatives of the ideal class group of K. Moreover, since $J_R(B_{\mathfrak{P}^{n+2}}) = J_R(B^{(d)}_{\mathfrak{P}^{n+2}})$, we conclude that

$$\phi_d(\mathfrak{a}) \equiv 1 \bmod \mathfrak{P}^{n+2} \quad \text{for all } \mathfrak{a} \in \mathscr{C}_n. \tag{9.5}$$

Note that, for any lattice $\mathscr{L}$ and any $\lambda \neq 0 \in \mathbb{C}$, we have $\mathcal{E}_1^*(\lambda z, \lambda\mathscr{L}) = \lambda^{-1}\mathcal{E}_1^*(z, \mathscr{L})$. Hence, summing the formula (9.3) over all $\mathfrak{a} \in \mathscr{C}_n$, and taking $\lambda = 1/(\sqrt{d}\chi_d(\mathfrak{a}))$, we immediately obtain the equation

$$\begin{aligned}&\sum_{\mathfrak{a}\in\mathscr{C}_n} \phi_d(\mathfrak{a})L_{R\mathfrak{q}}(\overline{\phi}_d, \gamma_{\mathfrak{a}}, 1)/\Omega_\infty(A)\\ &\quad= \sum_{\mathfrak{a}\in\mathscr{C}_n} \xi(\mathfrak{a}) \sum_{\sigma\in\mathrm{Gal}(K(\mathfrak{q}R)/H)} \left(\sqrt{d}\right)^{\sigma-1} \frac{1}{R\sqrt{-q}}\mathcal{E}_1^*\left(\frac{\xi(\mathfrak{a})\Omega_\infty(A)}{R\sqrt{-q}}, \mathcal{L}_{\mathfrak{a}}\right)^\sigma.\end{aligned} \tag{9.6}$$

Now the values $L_{R\mathfrak{q}}(\overline{\phi}_d, \gamma_{\mathfrak{a}}, 1)/\Omega_\infty(A)$ are independent of n since $\mathscr{C}_n$ is a complete set of representatives of the ideal class group of K. Thus, we conclude from (9.5) that the left-hand side of (9.6) converges v-adically as $n \to \infty$ to $L_{R\mathfrak{q}}(\overline{\phi}_d, 1)/\Omega_\infty(A)$, assuming R is fixed. Therefore, the right-hand side of (9.6) also converges v-adically as $n \to \infty$, and so we have proven the following result.

LEMMA 9.5. *For every positive integer divisor d of R, we have*

$$L_{R\mathfrak{q}}(\overline{\phi}_d, 1)/\Omega_\infty(A) = \lim_{n\to\infty} \sum_{\mathfrak{a}\in\mathscr{C}_n} \xi(\mathfrak{a}) \sum_{\sigma\in\mathrm{Gal}(K(R\mathfrak{q})/H)} \left(\sqrt{d}\right)^{\sigma-1} \frac{1}{R\sqrt{-q}}\mathcal{E}_1^*\left(\frac{\xi(\mathfrak{a})\Omega_\infty(A)}{R\sqrt{-q}}, \mathcal{L}_{\mathfrak{a}}\right)^\sigma. \tag{9.7}$$

One of the key idea in Zhao's induction method is to sum the formula (9.7) over all positive integer divisors d of R, and then make use of the following well-known lemma.

LEMMA 9.6. *Recall that $R = r_1 \dots r_k$, where the r_i are distinct prime numbers. Let σ be any element of $\mathrm{Gal}(K(R\mathfrak{q})/H)$. Then, letting d run over all positive integer divisors of R, the expression $\sum_{d|R}(\sqrt{d})^{\sigma-1}$ is equal to 2^k if $\sigma \in \mathrm{Gal}(K(R\mathfrak{q})/H_R)$, and is equal to 0 otherwise.*

Proof. We quickly recall the proof. The first assertion of the lemma is clear. To prove the second assertion, suppose that σ maps $j \geqslant 1$ elements of the set $\{\sqrt{r_1}, \dots, \sqrt{r_k}\}$ to minus themselves, and write $V(\sigma)$ for the subset consisting of all such elements. If d is any positive integer divisor of R, then σ will fix $\sqrt{d}$ if and only if d is a product of an even number of elements

of $V(\sigma)$ with an arbitrary number of elements of the complement of $V(\sigma)$ in $\{\sqrt{r_1}, \dots, \sqrt{r_k}\}$. Thus the total number of d such that $\sqrt{d}$ is fixed by σ is equal to

$$2^{k-j}((j,0) + (j,2) + (j,4) + \cdots) = 2^{k-1},$$

where (j,i) denotes the number of ways of choosing i objects from a set of j objects. Similarly, the total number of d such that σ maps $\sqrt{d}$ to $-\sqrt{d}$ is equal to

$$2^{k-j}((j,1) + (j,3) + (j,5) + \cdots) = 2^{k-1},$$

and the second assertion of the lemma is now clear. □

For each $\mathfrak{a} \in \mathscr{C}_n$, define

$$\Psi_{\mathfrak{a},R} = \mathrm{Tr}_{K(R\mathfrak{q})/H_R}\left(\frac{1}{R\sqrt{-q}} \cdot \mathcal{E}_1^*\left(\frac{\xi(\mathfrak{a})\Omega_\infty(A)}{R\sqrt{-q}}, \mathcal{L}_\mathfrak{a}\right)\right).$$

In view of the above lemma, it follows that Lemma 9.7 implies the following result.

PROPOSITION 9.7. *Letting d runs over all positive integer divisors of R, we have*

$$\sum_{d|R} L_{R\mathfrak{q}}(\overline{\phi}_d, 1)/\Omega_\infty(A) = 2^k \cdot \lim_{n\to\infty} \sum_{\mathfrak{a}\in\mathscr{C}_n} \xi(\mathfrak{a})\Psi_{\mathfrak{a},R}. \tag{9.8}$$

Finally, we shall need the following key integrality result (see [9, 11]).

PROPOSITION 9.8. *For all $\mathfrak{a} \in \mathscr{C}_n$, $\Psi_{\mathfrak{a},R}$ is integral at all places of H_R above 2.*

Proof. We briefly recall the proof given in [11]. Write $\mathfrak{J} = H(A^\mathfrak{a}_\mathfrak{q})$, which is also the ray class field $K(\mathfrak{q})$. Since $A^\mathfrak{a}$ is a relative Lubin–Tate formal group, in the sense of De Shalit [17], at each prime of H lying above the set of primes of K dividing R, it is easily seen that the action of the Galois group $\mathrm{Gal}(K(R\mathfrak{q})/\mathfrak{J})$ on $A^\mathfrak{a}_R$ gives an isomorphism

$$\tau : \mathrm{Gal}(K(R\mathfrak{q})/\mathfrak{J}) \simeq (\mathcal{O}_K/R\mathcal{O}_K)^\times.$$

Since q is prime to R, we can find α, β in $\mathcal{O}_K$ such that $1 = \alpha R + \beta\sqrt{-q}$. We then define

$$z_1 = \frac{\xi(\mathfrak{a})\alpha\Omega_\infty(A)}{\sqrt{-q}}, \quad z_2 = \frac{\xi(\mathfrak{a})\beta\Omega_\infty(A)}{R},$$

and write P_1 and P_2 for the corresponding points on $A^\mathfrak{a}$ under the Weierstrass isomorphism. For any $b \in H$, let $b^\mathfrak{a}$ denote the image of b under the Artin symbol of $\mathfrak{a}$. Define ϵ to be the inverse image of the class -1 mod $R\mathcal{O}_K$ under the isomorphism τ, and let $\mathfrak{S}$ be the fixed field of ϵ, so that the extension $K(R\mathfrak{q})/\mathfrak{S}$ has degree 2. Of course, $\mathfrak{S}$ contains H_R because -1 is a square modulo r_j for $j = 1, \dots k$. Defining $\Phi_\mathfrak{a} = \mathrm{Tr}_{K(R\mathfrak{q})/\mathfrak{S}}(\Psi_\mathfrak{a})$, we have

$$\Phi_\mathfrak{a} = \frac{1}{R\sqrt{-q}} \cdot (\mathcal{E}_1^*(z_1 + z_2, \mathcal{L}_\mathfrak{a}) + \mathcal{E}_1^*(z_1 - z_2, \mathcal{L}_\mathfrak{a}))$$

On the other hand, by a classical identity (see [11, Lemma 4.3]), we have

$$\mathcal{E}_1^*(z_1 + z_2, \mathcal{L}_\mathfrak{a}) + \mathcal{E}_1^*(z_1 - z_2, \mathcal{L}_\mathfrak{a}) = 2\mathcal{E}_1^*(z_1, \mathcal{L}_\mathfrak{a}) + \frac{2y(P_1) + a_1^\mathfrak{a} \cdot x(P_1) + a_3^\mathfrak{a}}{x(P_1) - x(P_2)}.$$

However, as is explained in detail in [11], each of the two terms on the right-hand side of this last equation is integral at all places of $\mathfrak{S}$ lying above 2, and the assertion of the lemma follows. □

As always, $\mathfrak{P}$ denotes the degree 1 prime of $\mathscr{T}$ lying above $\mathfrak{p}$ whose existence is given by Lemma 2.1, and we write $\mathscr{P}$ for any of the primes of the field $H\mathscr{T}$ lying above $\mathfrak{P}$. Now Proposition 9.3 shows that the value $\sqrt{R}L(\overline{\phi}_R, 1)/\Omega_\infty$ belongs to $H\mathscr{T}$ for all $R \in \mathscr{R}$.

THEOREM 9.9. *Assume $q \equiv 7 \bmod 16$, and let $R = r_1 \cdots r_k$ be any element of the set $\mathscr{R}$. Then, for each prime $\mathscr{P}$ of $H\mathscr{T}$ lying above the prime $\mathfrak{P}$ of $\mathscr{P}$, we have*

$$\operatorname{ord}_{\mathscr{P}}(\sqrt{R}L(\overline{\phi}_R, 1)/\Omega_\infty) = k - 1. \tag{9.9}$$

In particular, $L(\overline{\phi}_R, 1) \neq 0$.

We recall that we have taken an arbitrary embedding $i : \mathscr{T} \to \mathbb{C}$ in the above discussion, and each such ι then gives an embedding of $H\mathscr{T}$ into $\mathbb{C}$ because of our fixed embedding of H into $\mathbb{C}$. Since the above theorem holds for every choice of the h distinct embeddings of $\mathscr{T}$ into $\mathbb{C}$ extending the embedding of K into $\mathbb{C}$, we immediately obtain the following corollary, which establishes Theorem 1.3.

COROLLARY 9.10. *Assume that $q \equiv 7 \bmod 16$, and let R be any element of $\mathscr{R}$. Then $L(A^{(R)}/H, 1) \neq 0$.*

We prove Theorem 9.9 by induction on the number k of prime factors of R. We first establish some preliminary lemmas. Recall that $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, and that $F = K(B_{\mathfrak{P}^2})$. Then $\mathfrak{p}$ and $\mathfrak{q}$ are the only two primes of K which are ramified in the extension F/K. We thank Zhibin Liang for pointing out the following result to us.

LEMMA 9.11. *If $q \equiv 7 \bmod 16$, then $\mathfrak{p}^*$ is inert in F, and if $q \equiv 15 \bmod 16$, then $\mathfrak{p}^*$ splits in F.*

Proof. We recall that we have fixed the sign of $\alpha = \sqrt{-q}$ so that $\operatorname{ord}_{\mathfrak{p}}((1-\alpha)/2) > 0$. Then, by Lemma 7.11, we have $F = K(\sqrt{-\alpha})$. Thus F is the splitting field over K of the polynomial $g(X) = X^2 + X + (\alpha+1)/4$. Noting that

$$(1+\alpha)(1-\alpha)/4 = (q+1)/4, \quad (1+\alpha)/2 + (1-\alpha)/2 = 1,$$

it follows easily that $g(X)$ modulo $\mathfrak{p}^*$ is equal to $X^2 + X + 1$ if $q \equiv 7 \bmod 16$, and it is equal to $X^2 + X$ if $q \equiv 15 \bmod 16$. The assertions of the lemma now follow easily. □

COROLLARY 9.12. *If $q \equiv 7 \bmod 16$, then $\operatorname{ord}_{\mathfrak{P}}(\phi(\mathfrak{p}^*) - 1) = 1$, and if $q \equiv 15 \bmod 16$, then $\operatorname{ord}_{\mathfrak{P}}(\phi(\mathfrak{p}^*) - 1) \geqslant 2$.*

Proof. The prime $\mathfrak{p}^*$ is unramified in the extension F/K, and we let τ be its Artin symbol. Since ϕ is the Serre–Tate homomorphism for B/K, we have $\tau(Q) = \phi(\mathfrak{p}^*)(Q)$ for all Q in $B_{\mathfrak{P}^2}$, whence the assertion of the corollary follows from the previous lemma. □

LEMMA 9.13. *For each $R \in \mathscr{R}$, the extension J_R/K defined by (9.4) is unramified at the primes of K lying above 2.*

Proof. It suffices to show that, for each prime r dividing R, the extension $K(\sqrt{r})/K$ is unramified at the primes above 2. Put $m = (\sqrt{r} - 1)/2$, so that $V(m) = 0$, where $V(X) = X^2 + X - (r-1)/4$. But then $V'(m) = 2m - 1$ is a unit at $\mathfrak{p}$ and $\mathfrak{p}^*$, and so $K(m) = K(\sqrt{r})$ is unramified at the primes of K above 2. □

We first show that Theorem 9.9 holds for $R = 1$.

PROPOSITION 9.14. *Assume $q \equiv 7 \bmod 16$. Then, for all primes $\mathscr{P}$ of $H\mathscr{T}$ above $\mathfrak{P}$, we have* $\mathrm{ord}_{\mathscr{P}}(L(\overline{\phi},1)/\Omega_\infty(A)) = -1$.

Proof. The proof makes essential use of the so-called 'main conjecture' for B over the field $F_\infty = K(B_{\mathfrak{P}^\infty})$, which is given by Theorem 7.13. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$. Let $\mathscr{I}$ be the ring of integers of the completion of the maximal unramified extension of $K_\mathfrak{p}$, and write $\Lambda_\mathscr{I}(\Gamma)$ for the Iwasawa algebra of Γ with coefficients in $\mathscr{I}$. Then, as is explained in the proof of Corollary 7.15 the full force of the main conjecture tells us that the measure μ_A appearing in Theorem 7.13 is a unit in $\Lambda_\mathscr{I}(\Gamma)$ when $q \equiv 7 \bmod 16$. Hence the integral of any continuous homomorphism from Γ to $\mathscr{I}^\times$ against this measure must be a unit in $\mathscr{I}$. Thus, recalling that the $\mathfrak{p}$-adic period $\Omega_\mathfrak{p}(A)$ is a unit in $\mathscr{I}$, it follows from equation (7.20) that

$$\Omega_\infty(A)^{-1} L(\overline{\phi},1)(1-\phi(\mathfrak{p})/N\mathfrak{p})$$

will be a unit in $\mathscr{I}$, and thus a unit at $\mathfrak{Q}$. But, noting that $\phi(\mathfrak{p})\phi(\mathfrak{p}^*) = N\mathfrak{p}$, the conclusion of the proposition follows immediately from the first assertion of Corollary 9.12. □

We next consider the case when $k = 1$, and so $R = r$, a prime number. By Theorem 9.7 for the prime r, we conclude that

$$L(\overline{\phi}_r,1)/\Omega_\infty(A) + (1-\overline{\phi}((r))/r^2)L(\overline{\phi},1)/\Omega_\infty(A) = 2V_r, \tag{9.10}$$

where $V_r = \lim_{n\to\infty} \sum_{\mathfrak{a}\in\mathfrak{C}_n} \xi(\mathfrak{a})\Psi_{\mathfrak{a},r}$. Let $\mathfrak{W}$ be any prime of $H\mathscr{T}(\sqrt{r})$ lying above the prime $\mathfrak{P}$ of $\mathscr{T}$. By Proposition 9.8, we have $\mathrm{ord}_\mathfrak{W}(V_r) \geqslant 0$. Further, by Lemma 9.1, we have $(1-\overline{\phi}((r))/r^2) = (1+1/r)$. Thus, since $r+1 \equiv 2 \bmod 4$, it follows from Proposition 9.14 that $\mathrm{ord}_\mathfrak{W}((1-\overline{\phi}((r))/r^2)\mathscr{L}) = 0$. As $\mathrm{ord}_\mathfrak{W}(V_r) \geqslant 0$ by Proposition 9.8, we conclude from (9.10) that Theorem 9.9 holds when $k = 1$.

A curious new aspect of the argument now arises when we try to carry out the inductive argument for $k \geqslant 2$. For each positive divisor d of R, we define

$$\mathscr{L}(d) = \sqrt{d}L(\overline{\phi}_d,1)/\Omega_\infty(A),\ \ \mathscr{L} = \mathscr{L}(1). \tag{9.11}$$

Proposition 9.3 shows that $\mathscr{L}(d)$ always belongs to the field $H\mathscr{T}$, and $\mathscr{L} \neq 0$ by Proposition 9.14. However, the following stronger result is essential for our inductive argument.

PROPOSITION 9.15. *Assume $R \in \mathscr{R}$, and let d be any positive divisor of R. Then $\mathscr{L}(d)/\mathscr{L}$ belongs to the field $\mathscr{T}$.*

Proof. For each integral ideal $\mathfrak{a}$ of K, which is prime to $R\mathfrak{q}$, we define

$$e_\mathfrak{a} = \phi(\mathfrak{a})/\xi(\mathfrak{a}).$$

Then, as is already shown in [**19**] (see Corollary 4.11), $e_\mathfrak{a}$ only depends on the ideal class of $\mathfrak{a}$, and so, writing σ for the Artin symbol of $\mathfrak{a}$ in $\mathfrak{G} = \mathrm{Gal}(H/K)$, we put $e_\sigma = e_\mathfrak{a}$. Now let d be any positive divisor of R, so that $\mathscr{L}(d)$ belongs to the field $H\mathscr{T}$. Recall also that $\mathrm{Gal}(H\mathscr{T}/\mathscr{T})$ is isomorphic to $\mathrm{Gal}(H/K)$ under restriction, because $H \cap \mathscr{T} = K$. If τ is any element of $\mathrm{Gal}(H\mathscr{T}/\mathscr{T})$, we write τ_H for its restriction to H. Then it is proven in [**3**, Proposition 11.1] that, for every τ in $\mathrm{Gal}(H\mathscr{T}/\mathscr{T})$, we have

$$\tau(\mathscr{L}(d)) = e_{\tau_H}\mathscr{L}(d).$$

Since the factor e_{τ_H} is independent of d, it follows that $\mathscr{L}(d)/\mathscr{L}$ must belong to $\mathscr{T}$, and the proof is complete. □

Assume now that $R = r_1 \dots r_k$, where $k \geqslant 2$. By Theorem 9.7, we have

$$\mathscr{L}(R)/\sqrt{R} + \sum_{d|R, d\neq 1,R} \Lambda(d,R)/\sqrt{d} + \mathscr{L}\prod_{i=1}^{k}(1-\overline{\phi}((r_i))/r_i^2) = 2^k V_R, \tag{9.12}$$

where $V_R = \lim_{n\to\infty} \sum_{\mathfrak{a}\in\mathfrak{C}_n} \xi(\mathfrak{a})\Psi_{\mathfrak{a},R}$, and

$$\Lambda(d,R) = \mathscr{L}(d) \prod_{r|R/d} (1-\overline{\phi}_d((r))/r^2).$$

Now the terms $\Lambda(d,R)$ lie in an extension of $H\mathscr{T}$ where the prime $\mathfrak{P}$ of $\mathscr{T}$ is unramified but will usually have a large residue class field extension, and this means one cannot carry through the inductive argument in its most naive form. The key to overcoming this difficulty is to divide both side of (9.12) by the non-zero number $\mathscr{L}$. Doing this, and defining, for each positive integer divisor d of R, $\Phi(d,R) = \Lambda(d,R)/\mathscr{L}$, we obtain the equation

$$\Phi(R)/\sqrt{R} + \sum_{d|R, d\neq 1,R} \Phi(d,R)/\sqrt{d} + \prod_{i=1}^{k}(1-\overline{\phi}((r_i))/r_i^2) = 2^k V_R/\mathscr{L}, \tag{9.13}$$

where $\Phi(R) = \mathscr{L}(R)/\mathscr{L}$. Let H_R be the field defined in (9.4), and we now take $\mathfrak{W}$ to be any prime of the compositum $H_R\mathscr{T}$ lying above $\mathfrak{P}$, so that $\mathfrak{W}/\mathfrak{P}$ is unramified. By Proposition 9.8, we have $\mathrm{ord}_{\mathfrak{W}}(V_R) \geqslant 0$. Thus we conclude from Propositions 9.8 and 9.14 that $\mathrm{ord}_{\mathfrak{W}}(2^k V_R/\mathscr{L}) \geqslant k+1$. Thanks to Lemma 9.1, we have

$$\mathrm{ord}_{\mathfrak{W}}\left(\prod_{i=1}^{k}(1-\overline{\phi}((r_i))/r_i^2)\right) = k. \tag{9.14}$$

On the other hand, our inductive hypothesis, together with Lemma 9.1 and Proposition 9.14, shows that, for each positive divisor d of R, with $d \neq 1, R$, we have

$$\mathrm{ord}_{\mathfrak{W}}(\Phi(d,R)/\sqrt{d}) = k. \tag{9.15}$$

Of course, these estimates alone do not allow us to conclude from (9.13) that $\mathrm{ord}_{\mathfrak{W}}(\Phi(R)/\sqrt{R}) = k$. However, the argument is saved by Proposition 9.15, which tells us that, for every positive divisor d of R, $\Phi(d,R)$ belongs to the field $\mathscr{T}$, and so it lies in the completion $\mathscr{T}_{\mathfrak{P}}$ at $\mathfrak{P}$. Since $\mathfrak{P}$ has its residue field of order 2, this means that we can write, for every positive divisor $d \neq 1, R$ of R,

$$\Phi(d,R)/\sqrt{d} = \sqrt{d}\pi_{\mathfrak{P}}^k(1+\pi_{\mathfrak{P}}b_d), \tag{9.16}$$

where $\pi_{\mathfrak{P}}$ is a local parameter at $\mathfrak{P}$, and $\mathrm{ord}_{\mathfrak{P}}(b_d) \geqslant 0$. Thus

$$\sum_{d|R, d\neq 1,R} \Phi(d,R)/\sqrt{d} \equiv \pi_{\mathfrak{P}}^k D_R \bmod \mathfrak{W}^{k+1}, \tag{9.17}$$

with $D_R = \sum_{d|R.d\neq 1,R} \sqrt{d}$. But

$$D_R^2 \equiv \sum_{d|R.d\neq 1,R} d \bmod \mathfrak{W},$$

and $\sum_{d|R.d\neq 1,R} d \equiv 2^k \bmod 2$, whence $\mathrm{ord}_{\mathfrak{W}}(D_R) \geqslant 1$. Thus we have finally shown that

$$ord_{\mathfrak{W}}\left(\sum_{d|R, d\neq 1,R} \Phi(d,R)/\sqrt{d}\right) \geqslant k+1.$$

It now follows from (9.13) and (9.14) that $\mathrm{ord}_{\mathfrak{W}}(\Phi(R)) = k$. Thus, again using Proposition 9.14, we have finally proven Theorem 9.9 by induction on the number of prime factors of $R \in \mathscr{R}$.

We end this section with a numerical example. Take $q = 23$. Then $K = \mathbb{Q}(\sqrt{-23})$ has class number $h = 3$. The Hilbert class field is $H = K(\alpha)$, where α satisfies the equation $\alpha^3 - \alpha - 1 = 0$. The following global minimal Weierstrass equation for A/H is given by Gross [**21**]

$$y^2 + \alpha^3 xy + (\alpha + 2)y = x^3 + 2x^2 - (12\alpha^2 + 27\alpha + 16)x - (73\alpha^2 + 99\alpha + 62).$$

Then $\mathscr{R}$ will consist of all square free positive integers R such that every prime factor r of R satisfies $r \equiv 1 \bmod 4$ and r is congruent to one of $5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \bmod 23$. Then Theorem 1.3 shows that, for all $R \in \mathscr{R}$, we have $L(A^{(R)}/H, 1) \neq 0$. However, we thank Dabrowski for pointing out the following interesting numerical example to us. Let $\beta = \sqrt{-23}$, and define $\mathfrak{E}$ to be the elliptic curve defined over H, which is the twist of A/H by the quadratic extension $H(\sqrt{-\beta})/H$. Theorem 1.5 in the case $q = 23$ asserts that $L(\mathfrak{E}/H, 1) \neq 0$. Now take $R = 901 = 17 \times 53$, so that $R \in \mathfrak{R}$. Let $\mathfrak{E}^{(901)}/H$ be the twist of $\mathfrak{E}/H$ by the quadratic extension $H(\sqrt{901})/H$. Then Dabrowski's calculations show that $L(\mathfrak{E}^{(901)}/H, 1) = 0$. Thus the obvious analogue of Theorem 1.3 does not hold for the curve $\mathfrak{E}/H$.

Appendix

In this Appendix, we establish a strengthening of Theorem 5.4, and, for simplicity, we only treat the case $k = 1$, which is needed for our non-vanishing results. Let χ be an arbitrary non-trivial character of finite order of $G = \mathrm{Gal}(F_\infty/K)$. Let $\mathscr{T}_\chi$ be the field obtained by adjoining the values of χ to $\mathscr{T}$, and we fix an embedding of $\mathscr{T}_\chi$ into $\mathbb{C}$, which extends the embedding (2.2). As in § 4 and § 5, we fix an embedding of the compositum $H\mathscr{T}_\chi$ into the fraction field of $\mathscr{I}$ which induces our fixed prime w of H lying above $\mathfrak{p}$, and the prime $\mathfrak{P}$ of $\mathscr{T}$ above $\mathfrak{p}$. This is always possible because $H \cap \mathscr{T}_\chi = K$, since H does not contain any 2-power roots of unity of order greater than 2. Let $r \geqslant 0$ be the largest integer $\geqslant 0$ such that χ factors through $\mathrm{Gal}(F_r/K)$, so that the conductor $\mathfrak{g}_\chi$ of χ is equal to either $\mathfrak{q}\mathfrak{p}^{r+2}$ or $\mathfrak{p}^{r+2}$. Let ζ_r be the unique primitive 2^{r+2}-th root of unity such that $j_w(\zeta_r - 1) = t_w(V_r)$, where j_w is the isomorphism of formal groups given by (5.7), and V_r is the primitive $\mathfrak{p}^{r+2}$-division point on A defined at the end of § 2. Note that, for $\sigma \in \mathrm{Gal}(F_r/K)$, $\rho_{\mathfrak{P}}(\sigma)$ is a well-defined element of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{r+2})^\times$. We can then define the Gauss sum $\tau(\chi)$ by

$$\tau(\chi) = 2^{-(r+2)} \sum_{\sigma \in \mathrm{Gal}(F_r/K)} \zeta_r^{-\rho_{\mathfrak{P}}(\sigma)} \chi(\sigma). \tag{A.1}$$

It is readily verified that, since χ is non-trivial, we have $|\tau(\chi)| = 2^{r/2+1}$. Recall that $\mathcal{W}(z, \mathcal{L})$ denotes the Weierstrass isomorphism, and that Q denotes the primitive $\mathfrak{q}$-division point on A defined by (4.5). We fix a complex number z_χ such that $\mathcal{W}(z_\chi, \mathcal{L}) = V_r \oplus Q$. We will then have $(z_\chi/\Omega_\infty(A))\mathcal{O}_k = \mathfrak{h}_\chi/(\mathfrak{q}\mathfrak{p}^{r+2})$ for some integral ideal $\mathfrak{h}_\chi$ of K, which is prime to $\mathfrak{p}\mathfrak{q}$. For each $\alpha \in \mathscr{J}$, we let $\mu_{\alpha,\infty}$ be the $\mathscr{I}$-valued measure on G defined by (5.12). Write $L_\mathfrak{q}(\overline{\phi\chi}, s)$ for the Euler product of the Hecke L-function of $\overline{\phi\chi}$, but with the Euler factor at the prime $\mathfrak{q}$-removed.

THEOREM A.1. *For each non-trivial character χ of finite order of G, the value $\Omega_\infty(A)^{-1} L(\overline{\phi\chi}, 1)$ belongs to $H\mathscr{T}_\chi$, and we have*

$$\Omega_\mathfrak{p}(A)^{-1} \int_G \rho_{\mathfrak{P}} \chi d\mu_{\alpha,\infty} = \tau(\chi)(\phi\chi)(\mathfrak{h}_\chi) z_\chi^{-1} (N\alpha - (\phi\chi)((\alpha))) L_\mathfrak{q}(\overline{\phi\chi}, 1). \tag{A.2}$$

Proof. We fix a set $\mathcal{B}$ of integral ideals $\mathfrak{b}$ of K, prime to $\mathfrak{p}\mathfrak{q}$ such that

$$\mathrm{Gal}(F_r/K) = \{\tau_\mathfrak{b} | F_r : \mathfrak{b} \in \mathcal{B}\}, \tag{A.3}$$

where we recall that $\tau_{\mathfrak{b}}$ denotes the Artin symbol of $\mathfrak{b}$ in $\mathrm{Gal}(\mathfrak{F}_\infty/K)$. Recall that $\rho_{\mathfrak{P}}(\mathrm{Gal}(F_\infty/F_r)) = 1 + 2^{r+2}\mathcal{O}_{\mathfrak{p}}$, and note that the characteristic function $\gamma_r(x)$ of $1 + 2^{r+2}\mathcal{O}_{\mathfrak{p}}$ in $\mathcal{O}_{\mathfrak{p}}$ is given explicitly by

$$\gamma_r(x) = 2^{-(r+2)} \sum_{j \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{r+2}} \zeta_r^{(x-1)j}. \tag{A.4}$$

For $r \leqslant n \leqslant \infty$, the measure $\mu_{\alpha,n,w}$ in $\Lambda_{\mathscr{I}}(G)$ arises, via the isomorphism (5.5) and Mahler's theorem, from the power series $J_{\alpha,n,w}(t_w)$ defined in Lemma 5.3. For every $\sigma \in G$, we write $\mu^{(\sigma)}_{\alpha,n,w}$ for the measure $\sigma\mu_{\alpha,n,w}$, and note that $\mu^{(\sigma)}_{\alpha,n,w}$ arises, again via the isomorphism (5.5) and Mahler's theorem, from the power series $J^{(\sigma)}_{\alpha,n,w}(t_w)$ defined by

$$J^{(\sigma)}_{\alpha,n,w}(t_w) = J_{\alpha,n,w}(\widehat{\rho_{\mathfrak{p}}(\sigma)}_w(t_w)). \tag{A.5}$$

In what follows, for simplicity, we shall drop the fixed place w of H from the notation, and also we will just write $\mu^{\mathfrak{b}}_{\alpha,n}$ for the measure $(\tau_{\mathfrak{b}}|F_\infty)\mu_{\alpha,n,w}$. As usual, we write $\chi(\mathfrak{b}^{-1})$ for $\chi(\tau_{\mathfrak{b}}^{-1})$ when $\mathfrak{b} \in \mathcal{B}$, and we note that, due to our fixed embedding of $\mathscr{T}$ into the fraction field of $\mathscr{I}$, we have $\rho_{\mathfrak{P}}(\tau_{\mathfrak{b}}) = \phi(\mathfrak{b})$. It then follows easily from Mahler's theorem that

$$\int_G \rho_{\mathfrak{P}}\chi d\mu_{\alpha,n} = \sum_{\mathfrak{b}\in\mathcal{B}} (\phi\chi)(\mathfrak{b}^{-1}) \int_{\mathcal{O}_{\mathfrak{p}}} x\gamma_r(x) d\mu^{\mathfrak{b}}_{\alpha,n}.$$

Substituting the formula (A.4) for $\gamma_r(x)$ in the integral on the right-hand side, we conclude that

$$\int_G \rho_{\mathfrak{P}}\chi d\mu_{\alpha,n} = 2^{-(r+2)} \sum_{\mathfrak{b}\in\mathcal{B}} (\phi\chi)(\mathfrak{b}^{-1}) \sum_{j \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{r+2}} \int_{\mathcal{O}_{\mathfrak{p}}} \zeta_r^{(x-1)j} x d\mu^{\mathfrak{b}}_{\alpha,n}. \tag{A.6}$$

We omit the proof of the following classical lemma about the Mahler map $\mathbb{M}$ which is defined earlier immediately below (5.10). Let Δ denote the differential operator on $\mathscr{I}[[W]]$ defined by $\Delta f(W) = (1+W)d/dW\, f(W)$.

Lemma A.2. *Let μ be any element of $\Lambda_{\mathscr{I}}(\mathcal{O}_{\mathfrak{p}})$, and let $\mathbb{M}(\mu)$ be its Mahler power series in $\mathscr{I}[[W]]$. Then, if ζ denotes any 2-power root of unity, we have*

$$\Delta(\mathbb{M}(\mu))(\zeta - 1) = \int_{\mathcal{O}_{\mathfrak{p}}} x\zeta^x d\mu. \tag{A.7}$$

Now $\mathbb{M}(\mu^{\mathfrak{b}}_{\alpha,n}) = \mathfrak{K}_{\alpha,n,w,\mathfrak{b}}(W)$, where

$$\mathfrak{K}_{\alpha,n,w,\mathfrak{b}}(W) = J_{\alpha,n,w}(j_w((1+W)^{\phi(\mathfrak{b})} - 1)). \tag{A.8}$$

It then follows from the previous lemma that

$$\int_G \rho_{\mathfrak{P}}\chi d\mu_{\alpha,n} = 2^{-(r+2)} \sum_{j \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{r+2}} \zeta_r^{-j} \mathfrak{S}_r(j), \tag{A.9}$$

where

$$\mathfrak{S}_r(j) = \sum_{\mathfrak{b}\in\mathcal{B}} (\phi\chi)(\mathfrak{b}^{-1})(\Delta\mathfrak{K}_{\alpha,n,w,\mathfrak{b}})(\zeta_r^j - 1). \tag{A.10}$$

Lemma A.3. *If 2 divides j, then $\mathfrak{S}_r(j) = 0$.*

Proof. In view of the definition A.8, we see immediately that

$$\mathfrak{S}_r(j) = \sum_{\mathfrak{b}\in\mathcal{B}} \chi(\mathfrak{b}^{-1}) \frac{d}{dW}(J_{\alpha,n,w} \circ j_w)(\zeta_r^{\phi(\mathfrak{b})j} - 1)\zeta_r^{\phi(\mathfrak{b})j}. \tag{A.11}$$

Note that ζ_r^j is a 2^{r+1}-th root of unity if 2 divides j. Now the restriction of the character χ to $\mathrm{Gal}(F_r/F_{r-1})$ is not the trivial character by the definition of r; here we have put $F_{-1} = K$ if $r = 0$. Thus we have $\sum_{\sigma\in\mathrm{Gal}(F_r/F_{r-1})} \chi(\sigma) = 0$. On the other hand, we have $\phi(\mathfrak{b}_1) \equiv \phi(\mathfrak{b}_2) \bmod \mathfrak{P}^{r+1}$ if the restrictions of $\tau_{\mathfrak{b}_1}$ and $\tau_{\mathfrak{b}_2}$ to F_{r-1} are equal. The assertion of the lemma is now clear from the explicit expression (A.11) for $\mathfrak{S}_r(j)$. □

Lemma A.4. *We have*

$$\int_G \rho_{\mathfrak{P}}\chi d\mu_{\alpha,n} = \tau(\chi) \sum_{\mathfrak{b}\in\mathcal{B}} (\phi\chi)(\mathfrak{b}^{-1})(\Delta\mathfrak{K}_{\alpha,n,w,\mathfrak{b}})(\zeta_r - 1). \tag{A.12}$$

Proof. Define

$$W(\mathcal{B}) = \sum_{\mathfrak{b}\in\mathcal{B}} (\phi\chi)(\mathfrak{b}^{-1})(\Delta\mathfrak{K}_{\alpha,n,w,\mathfrak{b}})(\zeta_r - 1).$$

We claim that $W(\mathcal{B})$ is independent of the choice of the set $\mathcal{B}$ of integral ideals of K, prime to $\mathfrak{pq}$ such that $\mathrm{Gal}(F_r/K) = \{\tau_{\mathfrak{b}}|F_r : \mathfrak{b} \in \mathcal{B}\}$. Indeed, we have

$$W(\mathcal{B}) = \sum_{\mathfrak{b}\in\mathcal{B}} \chi(\mathfrak{b}^{-1}) \frac{d}{dW}(J_{\alpha,n,w} \circ j_w)(\zeta_r^{\phi(\mathfrak{b})} - 1)\zeta_r^{\phi(\mathfrak{b})}.$$

Now, if $\mathcal{B}'$ is another set of integral ideals of K with the above properties, then, for each $\mathfrak{b} \in \mathcal{B}$ there exists a unique $\mathfrak{b}' \in \mathcal{B}'$ such that $\tau_{\mathfrak{b}}|F_r = \tau_{\mathfrak{b}'}|F_r$. Then we have $\phi(\mathfrak{b}) \equiv \phi(\mathfrak{b}') \bmod \mathfrak{P}^{r+2}$, so that $\zeta_r^{\phi(\mathfrak{b})} = \zeta_r^{\phi(\mathfrak{b}')}$, whence it is clear that $W(\mathcal{B}) = W(\mathcal{B}')$. Now choose a set $\mathcal{E}$ of integral ideals of K, which are prime to $\mathfrak{pq}$, which are indexed by the odd integers j, with $1 \leqslant j < 2^{r+2}$, in such a way that $\phi(\mathfrak{e}_j) \equiv j \bmod \mathfrak{P}^{r+2}$. Then we clearly have

$$\zeta_r^{-j}\mathfrak{S}_r(j) = \chi(\mathfrak{e}_j)\zeta_r^{-\phi(\mathfrak{e}_j)}W(\mathcal{B}_j), \tag{A.13}$$

where $\mathcal{B}_j = \{\mathfrak{b}\mathfrak{e}_j : \mathfrak{b} \in \mathcal{B}\}$. But, from our previous remark, we have $W(\mathcal{B}_j) = W(\mathcal{B})$ for all odd integers j with $1 \leqslant j < 2^{r+2}$, and (A.12) follows. □

We recall that $j_w(\zeta_r - 1) = t_w(V_r)$, where $V_r \in A_{\mathfrak{p}^{r+2}}$ is defined at the end of § 2, and for simplicity, put $Q_r = V_r \oplus Q$. Moreover, we have fixed a complex number z_χ such that $\mathcal{W}(z_\chi, \mathcal{L}) = Q_r$, and then the integral ideal $\mathfrak{h}_\chi$ satisfies $(z_\chi/\Omega_\infty(A))\mathcal{O}_k = \mathfrak{h}_\chi/(\mathfrak{q}\mathfrak{p}^{r+2})$. If $\mathfrak{b}$ is any integral ideal of K prime to $\mathfrak{pq}$, we shall write $\tau_r(\mathfrak{b})$ for the restriction of the Artin symbol $\tau_{\mathfrak{b}}$ of $\mathfrak{b}$ to the subfield $\mathfrak{F}_r$ of $\mathfrak{F}_\infty$. Moreover, for such an ideal $\mathfrak{b}$, we define now the partial L-series for the extension F_r/K by

$$L_{\mathfrak{q}}(\overline{\phi}^k, \tau_r(\mathfrak{b}), s) = \sum_{\tau_r(\mathfrak{a})=\tau_r(\mathfrak{b})} \frac{\overline{\phi}^k(\mathfrak{a})}{(N(\mathfrak{a}))^s}, \tag{A.14}$$

where the sum is taken over all integral ideals $\mathfrak{a}$ of K, which are prime to $\mathfrak{pq}$, and which satisfy $\tau_r(\mathfrak{a}) = \tau_r(\mathfrak{b})$. Note that this is a different partial L-series from that defined by (5.14). We then have the following analogue of Proposition 5.5. Let $z_r \in \mathbb{C}$ be such that $\mathcal{W}(z_r, \mathcal{L}) = V_r$.

PROPOSITION A.5. *For all integral ideals $\mathfrak{d}$ of K, which are prime to $\mathfrak{pq}$, we have*

$$\frac{d}{dz}\log \mathfrak{R}_{\alpha,A^{\mathfrak{d}}}(\eta_A(\mathfrak{d})(\mathcal{W}(z+z_r,\mathcal{L}))=\sum_{k\geqslant 1}(-1)^{k-1}(\phi(\mathfrak{d}\mathfrak{h}_\chi)/z_\chi)^k(N\alpha L_{\mathfrak{q}}(\overline{\phi}^k,\tau_r(\mathfrak{d}\mathfrak{h}_\chi),k)$$
$$-\phi((\alpha))L_{\mathfrak{q}}(\overline{\phi}^k,\tau_r(\mathfrak{d}\mathfrak{h}_\chi(\alpha)),k))z^{k-1}. \tag{A.15}$$

Proof. It follows immediately from (5.16), (5.17), (5.19) that, for all complex numbers ζ, and all integral ideals $\mathfrak{d}$ of K prime to $\mathfrak{pq}$, we have

$$\frac{d}{dz}\log R_{\alpha,A^{\mathfrak{d}}}(\eta_A(\mathfrak{d})(\mathcal{W}(z+\zeta,\mathcal{L})))=\sum_{k\geqslant 1}(-1)^{k-1}\xi(\mathfrak{d})^k(N\alpha\mathcal{E}_k^*(\xi(\mathfrak{d})\zeta,\mathcal{L}_{\mathfrak{d}})$$
$$-\mathcal{E}_k^*(\xi(\mathfrak{d})\zeta,\alpha^{-1}\mathcal{L}_{\mathfrak{d}})z^{k-1}. \tag{A.16}$$

We now fix a set $\mathfrak{S}$ of integral ideals of K prime to $\mathfrak{pq}$ such that $\mathrm{Gal}(H(A_{\mathfrak{q}\mathfrak{p}^{r+2}})/\mathfrak{F}_r)=\{\tau'_{\mathfrak{s}}|H(A_{\mathfrak{q}\mathfrak{p}^{r+2}}):\mathfrak{s}\in\mathfrak{S}\}$; here we have written $\tau'_{\mathfrak{s}}$ for the Artin symbol of $\mathfrak{s}$ in $\mathrm{Gal}(H(A_{\mathfrak{q}\mathfrak{p}^\infty})/K$. All of the ideals $\mathfrak{s}\in\mathfrak{S}$ are norms of ideals of H because their Artin symbols fix the Hilbert class field H of K. Also, the Artin symbols of the ideals $\mathfrak{s}\in\mathfrak{S}$ fix the point V_r, and $\mathrm{Gal}(H(A_{\mathfrak{q}\mathfrak{p}^{r+2}})/\mathfrak{F}_r)$ is isomorphic to $\mathrm{Gal}(H(A_{\mathfrak{q}})/H)$ under restriction. It follows easily that

$$\frac{d}{dz}\log(\mathfrak{R}_{\alpha,A^{\mathfrak{d}}}(\eta_A(\mathfrak{d})(\mathcal{W}(z+z_r,\mathcal{L})))=\sum_{\mathfrak{s}\in\mathfrak{S}}\frac{d}{dz}(\log R_{\alpha,A^{\mathfrak{d}}}(\eta_A(\mathfrak{d})(\mathcal{W}(z+\phi(\mathfrak{s})z_\chi,\mathcal{L}))). \tag{A.17}$$

Hence we conclude from (A.16) that the right-hand side of (A.17) is equal to

$$\sum_{k\geqslant 1}(-1)^{k-1}\xi(\mathfrak{d})^k\sum_{\mathfrak{s}\in\mathfrak{S}}(N\alpha\mathcal{E}_k^*(\xi(\mathfrak{d})\phi(\mathfrak{s})z_\chi,\mathcal{L}_{\mathfrak{d}})-\mathcal{E}_k^*(\xi(\mathfrak{d})\phi(\mathfrak{s})z_\chi,\alpha^{-1}\mathcal{L}_{\mathfrak{d}}))z^{k-1}. \tag{A.18}$$

On the other hand, noting that

$$z_\chi\Omega_\infty(A)^{-1}\mathcal{O}_K=\mathfrak{h}_\chi/(\mathfrak{q}\mathfrak{p}^{r+2}),\ \alpha z_\chi\Omega_\infty(A)^{-1}\mathcal{O}_K=(\alpha)\mathfrak{h}_\chi/(\mathfrak{q}\mathfrak{p}^{r+2}),$$

we deduce from [**19**, Proposition 5.5] that

$$\sum_{\mathfrak{s}\in\mathfrak{S}}\mathcal{E}_k^*(\xi(\mathfrak{d})\phi(\mathfrak{s})z_\chi,\mathcal{L}_{\mathfrak{d}})=(\phi(\mathfrak{d}\mathfrak{h}_\chi)/\xi(\mathfrak{d})z_\chi)^kL_{\mathfrak{q}}(\overline{\phi}^k,\tau_r(\mathfrak{d}\mathfrak{h}_\chi),k),$$
$$\sum_{\mathfrak{s}\in\mathfrak{S}}\mathcal{E}_k^*(\xi(\mathfrak{d})\phi(\mathfrak{s})z_\chi,\alpha^{-1}\mathcal{L}_{\mathfrak{d}})=(\phi((\alpha)\mathfrak{d}\mathfrak{h}_\chi)/\xi(\mathfrak{d})z_\chi)^kL_{\mathfrak{q}}(\overline{\phi}^k,\tau_r((\alpha)\mathfrak{d}\mathfrak{h}_\chi),k).$$

Substituting these last two expressions into (A.18), equation (A.15) follows, and the proof of Proposition A.5 is complete. □

Moreover, putting $z=0$ in (A.12), we obtain the following corollary.

COROLLARY A.6. *For all integral ideals $\mathfrak{d}$ of K, which are prime to $\mathfrak{pq}$, we have*

$$\frac{d}{dz}\log \mathfrak{R}_{\alpha,A^{\mathfrak{d}}}(\eta_A(\mathfrak{d})\mathcal{W}(z,\mathcal{L}))|_{z=z_r}=\phi(\mathfrak{d}\mathfrak{h}_\chi){z_\chi}^{-1}(N\alpha L_{\mathfrak{q}}(\overline{\phi},\tau_r(\mathfrak{d}\mathfrak{h}_\chi),1)$$
$$-\phi((\alpha))L_{\mathfrak{q}}(\overline{\phi},\tau_r(\mathfrak{d}\mathfrak{h}_\chi(\alpha)),1)).$$

Recalling that $\mathrm{Gal}(\mathfrak{F}_r/H)$ is isomorphic under restriction to $\mathrm{Gal}(F_r/K)$, we assume from now on that that we have chosen the set $\mathcal{B}$ of integral ideals of K, prime to $\mathfrak{pq}$, such that

$$\mathrm{Gal}(\mathfrak{F}_r/H)=\{\tau_r(\mathfrak{b}):\mathfrak{b}\in\mathcal{B}\}. \tag{A.19}$$

Now take n to be any finite integer $\geqslant r$, and let $\mathfrak{C}_n$ be the set of integral ideals of K, prime to $\mathfrak{pq}$, satisfying (2.12). Since $\mathrm{Gal}(\mathfrak{F}_n/K_n)$ is isomorphic to $\mathrm{Gal}(\mathfrak{F}_r/F_r)$ under restriction, it follows that

$$\mathrm{Gal}(\mathfrak{F}_r/K) = \{\tau_r(\mathfrak{bc}) : \mathfrak{b} \in \mathcal{B}, \mathfrak{c} \in \mathfrak{C}_n\}. \tag{A.20}$$

Now, for $\mathfrak{b} \in \mathcal{B}$, we have $\Delta\mathfrak{K}_{\alpha,n,w,\mathfrak{b}}(W) = \Phi_{1,n,\mathfrak{b}}(W) - \Phi_{2,n,\mathfrak{b}}(W)$, where

$$\begin{aligned}\Phi_{1,n,\mathfrak{b}}(W) &= \Delta\log(d_{\alpha,n}(j_w((1+W)^{\phi(\mathfrak{b})}-1))),\ \Phi_{2,n,\mathfrak{b}}(W)\\ &= \tfrac{1}{2}\Delta\log(d^{\delta}_{\alpha,n}(\widehat{\eta_{A,\mathfrak{p},w}}(j_w((1+W)^{\phi(\mathfrak{b})}-1)))).\end{aligned} \tag{A.21}$$

Lemma A.7. *For every integer $n \geqslant r$, we have*

$$\sum_{\mathfrak{b}\in\mathcal{B}}(\phi\chi)(\mathfrak{b}^{-1})\Phi_{1,n,\mathfrak{b}}(\zeta_r-1) = \Omega_{\mathfrak{p}}(A)\phi(\mathfrak{h}_\chi)z_\chi^{-1}\sum_{\mathfrak{b}\in\mathcal{B}}\chi(\mathfrak{b}^{-1})\sum_{\mathfrak{c}\in\mathfrak{C}_n}\phi(\mathfrak{c})(N\alpha L_{\mathfrak{q}}(\overline{\phi},\tau_r(\mathfrak{bch}_\chi),1)$$
$$-\phi((\alpha))L_{\mathfrak{q}}(\overline{\phi},\tau_r((\alpha)\mathfrak{bch}_\chi),1)).$$

Proof. Let $\mathfrak{b}$ be any element of $\mathcal{B}$. Since $\tau_r(\mathfrak{b})$ fixes H, we see that $A^{\mathfrak{b}} = A^{\mathfrak{bc}}$, whence it follows easily from (4.15) that $\Phi_{1,n,\mathfrak{b}}(W)$ is obtained by first substituting $t_w = j_w(W)$ in the t_w-expansion of the rational function on A/H given by

$$\prod_{\mathfrak{c}\in\mathfrak{C}_n}\mathfrak{R}_{\alpha,A^{\mathfrak{cb}}}(\eta_A(\mathfrak{cb})(P)),$$

and then applying the operator Δ to the logarithm of this series in W. Hence, recalling (5.23) and the fact that $V_r = j_w(\zeta_r - 1)$, we conclude that

$$\Phi_{1,n,\mathfrak{b}}(W)(\zeta_r-1) = \Omega_{\mathfrak{p}}(A)\sum_{\mathfrak{c}\in\mathfrak{C}_n}\frac{d}{dz}\log\mathfrak{R}_{\alpha,A^{\mathfrak{cb}}}(\eta_A(\mathfrak{cb})\mathcal{W}(z,\mathcal{L}))|_{z=z_r},$$

and so the assertion of the lemma is now clear from Corollary A.6. □

Lemma A.8. *For every integer $n \geqslant r$, we have*

$$\sum_{\mathfrak{b}\in\mathcal{B}}(\phi\chi)(\mathfrak{b}^{-1})\Phi_{2,n,\mathfrak{b}}(\zeta_r-1) = 0. \tag{A.22}$$

Proof. For each $\mathfrak{b} \in \mathcal{B}$, we have

$$2\Phi_{2,n,\mathfrak{b}}(\zeta_r-1) = \Omega_{\mathfrak{p}}(A)\frac{d}{dz}(\log D^{\delta}_{\alpha,n}(\eta_A^{\mathfrak{p}}(\mathfrak{b})\eta_A(\mathfrak{p})(P)))|_{P=V_r}.$$

Recalling that, by (2.13), we have $\eta_A(\mathfrak{p})(V_r) = V^{\delta}_{r-1}$, and noting that $A^{\mathfrak{pb}} = A^{\mathfrak{p}}$ because $\tau_r(\mathfrak{b})$ acts trivially on H, it follows that

$$2\Phi_{2,n,\mathfrak{b}}(\zeta_r-1) = \Omega_{\mathfrak{p}}(A)\phi(\mathfrak{bp})\frac{d}{dz}(\log D^{\delta}_{\alpha,n}(P))|_{P=\eta_{A^{\mathfrak{p}}}(\mathfrak{b})(V^{\delta}_{r-1})}. \tag{A.23}$$

Hence we have

$$2\sum_{\mathfrak{b}\in\mathcal{B}}(\phi\chi)(\mathfrak{b}^{-1})\Phi_{2,n,\mathfrak{b}}(\zeta_r-1) = \phi(\mathfrak{p})\sum_{\mathfrak{b}\in\mathcal{B}}\chi(\mathfrak{b}^{-1})\frac{d}{dz}(\log D^{\delta}_{\alpha,n}(P))|_{P=\eta_{A^{\mathfrak{p}}}(\mathfrak{b})(V^{\delta}_{r-1})}. \tag{A.24}$$

Let $\mathcal{B}'$ be the subset of all those $\mathfrak{b} \in \mathcal{B}$ such that $\tau_r(\mathfrak{b})$ fixes $\mathfrak{F}_{r-1}$. Then $\eta_{A^{\mathfrak{p}}}(\mathfrak{b})(V^{\delta}_{r-1}) = V^{\delta}_{r-1}$ for $\mathfrak{b} \in \mathcal{B}'$, and $\sum_{\mathfrak{b}\in\mathcal{B}'}\chi(\mathfrak{b}^{-1}) = 0$ because the restriction of χ to $\mathrm{Gal}(F_r/F_{r-1})$ is non-trivial. Using these facts, the assertion (A.22) follows easily from (A.24). □

We can now at last complete the proof of Theorem A.1. Combining Lemmas A.4, A.7, A.8, we see that, for each finite integer $n \geqslant r$, we have

$$\Omega_{\mathfrak{p}}(A)^{-1} \int_G \rho_{\mathfrak{P}} \chi d\mu_{\alpha,n} = \tau(\chi)\phi(\mathfrak{h}_\chi) z_\chi^{-1} \sum_{\mathfrak{b} \in \mathcal{B}} \chi(\mathfrak{b}^{-1}) \sum_{\mathfrak{c} \in \mathfrak{C}_n} \phi(\mathfrak{c}) (N\alpha L_{\mathfrak{q}}(\overline{\phi}, \tau_r(\mathfrak{bch}_\chi), 1)$$

$$- \phi((\alpha)) L_{\mathfrak{q}}(\overline{\phi}, \tau_r((\alpha)\mathfrak{bch}_\chi), 1)). \tag{A.25}$$

Note also that Corollary A.6 shows that, for all $\mathfrak{c} \in \mathfrak{C}_n$ and $\mathfrak{b} \in \mathcal{B}$, the expression $z_\chi^{-1}(N\alpha L_{\mathfrak{q}}(\overline{\phi}, \tau_r(\mathfrak{bch}_\chi), 1) - \phi((\alpha)) L_{\mathfrak{q}}(\overline{\phi}, \tau_r((\alpha)\mathfrak{bch}_\chi), 1))$ is integral at our fixed embedding of $H\mathscr{T}$ in the fraction field of $\mathscr{I}$. Now, letting $n \to \infty$, the left-hand side of (A.25) converges to $\Omega_{\mathfrak{p}}(A)^{-1} \int_G \rho_{\mathfrak{P}} \chi d\mu_{\alpha,\infty}$. Recalling that $\phi(\mathfrak{c}) \equiv 1 \bmod \mathfrak{P}^{n+2}$ for all $\mathfrak{c} \in \mathfrak{C}_n$, it is clear that the right-hand side of (A.25) converges to $\tau(\chi)(\phi\chi)(\mathfrak{h}_\chi) z_\chi^{-1}(N\alpha - (\phi\chi)((\alpha))) L_{\mathfrak{q}}(\overline{\phi\chi}, 1)$, and the proof of Theorem A.1 is complete. □

References

1. W. Berwick, 'Modular invariants expressible in terms of quadratic and cubic irrationalities', *Proc. Lond. Math. Soc.* (2) 28 (1928) 53–69.
2. B. Birch, 'Diophantine analysis and modular functions', *Algebr. Geom. Bombay Colloq.* (1968) 35–42.
3. J. Buhler and B. Gross, 'Arithmetic on elliptic curves with complex multiplication II', *Invent. Math.* 79 (1985) 11–29.
4. J. Choi, 'Iwasawa μ-invariants and elliptic curves with complex multiplication', PhD Thesis, POSTECH, 2018.
5. J. Choi and J. Coates, 'Iwasawa theory of quadratic twists of $X_0(49)$', *Acta Math. Sin.* (*Engl. Ser.*) 34 (2017) 19–28.
6. J. Choi, Y. Kezuka and Y. Li, 'Analogues of Iwasawa's $\mu = 0$ conjecture and weak Leopoldt theorem for certain non-cyclotomic $\mathbb{Z}_2$-extensions', *Asian J. Math.* 23 (2019) 383–400.
7. J. Coates, 'Infinite descent on elliptic curves with complex multiplication', *Arithmetic and geometry*, vol. I, Progress in Mathematics 35 (eds M. Artin and J. Tate; Birkhauser Boston, Boston, MA, 1983) 107–137.
8. J. Coates, 'Elliptic curves with complex multiplication and Iwasawa theory', *Bull. Lond. Math. Soc.* 23 (1991) 321–350.
9. J. Coates, 'Lectures on the Birch-Swinnerton-Dyer conjecture', *ICCM Not.* 1 (2013) 29–46.
10. J. Coates, Y. Kezuka, Y. Li and Y. Tian, 'On the Birch-Swinnerton-Dyer Conjecture for certain elliptic curves with complex multiplication', in preparation.
11. J. Coates, Y. Li, Y. Tian and S. Zhai, 'Quadratic twists of elliptic curves', *Proc. Lond. Math. Soc.* (3) 110 (2015) 357–394.
12. J. Coates and R. Sujatha, *Cyclotomic fields and zeta values*, Springer Monographs in Mathematics (Springer, Berlin, 2006).
13. J. Coates and A. Wiles, 'Kummer's criterion for Hurwitz numbers', *Algebraic number theory* (ed. S. Iyanaga; Japan Society for the Promotion of Science, Tokyo, 1977) 9–23.
14. J. Coates and A. Wiles, 'On p-adic L-functions and elliptic units', *J. Aust. Math. Soc.* 26 (1978) 1–25.
15. A. Dabrowski, T. Jedrzejak and L. Szymaszkiewicz, 'Critical L-values for some quadratic twists of Gross curves', *Asian J. Math.*, to appear.
16. A. Dabrowski, T. Jedrzejak and L. Szymaszkiewicz, 'Critical L-values of Gross curves', Preprint, 2019, arXiv:1904.08691.
17. E. de Shalit, 'Relative Lubin-Tate groups', *Proc. Amer. Math. Soc.* 95 (1985) 1–4.
18. E. de Shalit, *The Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics 3 (Academic Press, Cambridge, MA, 1987).
19. C. Goldstein and N. Schappacher, 'Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe', *J. reine angew. Math.* 327 (1981) 184–218.
20. R. Greenberg, 'On the structure of certain Galois groups', *Invent. Math.* 47 (1978) 85–99.
21. B. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics 776 (Springer, Berlin, 1980).
22. B. Gross, 'Minimal models for elliptic curves with complex multiplication', *Compos. Math.* 45 (1982) 155–164.
23. K. Iwasawa, 'On some modules in the theory of cyclotomic fields', *J. Math. Soc. Japan* 16 (1964) 42–82.
24. K. Kato, 'p-adic Hodge theory and values of zeta functions of modular forms', *Asterisque* 295 (2004) 117–290.
25. J. Li, 'On the 2-adic logarithm of units of pure imaginary quartic fields', *Asian J. Math.*, to appear.
26. K. Li and Y. Ren, 'On the quadratic twists of Gross curves', *J. Sichuan Normal Univ.* 39 (2016) 37–46.
27. B. Perrin-Riou, 'Arithmetique des courbes elliptiques et theorie d'Iwasawa', *Mem. Soc. Math. de France, fascicule* 4 112 (1984).

28. D. Rohrlich, 'The non-vanishing of certain Hecke L-functions at the center of the critical strip', *Duke Math. J.* 47 (1980) 223–232.
29. D. Rohrlich, 'L-functions and division towers', *Math. Ann.* 281 (1988) 611–632.
30. J-P. Serre and J. Tate, 'Good reduction of abelian varieties', *Ann. of Math.* (2) 88 (1968) 492–517.
31. C. Zhao, 'A criterion for elliptic curves with lowest 2-power in $L(1)$', *Math. Proc. Cambridge Philos. Soc.* 121 (1997) 385–400.
32. C. Zhao, 'A criterion for elliptic curves with second lowest 2-power in $L(1)$', *Math. Proc. Cambridge Philos. Soc.* 131 (2001) 385–404.

John Coates
Emmanuel College
Cambridge
England

jhc13@dpmms.cam.ac.uk

Yongxiong Li
Yau Mathematical Sciences Center
Tsinghua University
Beijing
China

liyx_1029@mail.tsinghua.edu.cn